2001

CPA's handbook of fraud and commercial crime prevention

Tedd Avey

Ted Baskerville

Alan Brill

The CPA's Handbook of Fraud and Commercial Crime Prevention

AICPA

American Institute of Certified Public Accountants

The CPA's Handbook of Fraud and Commercial Crime Prevention

AICPA

Tedd Avey, CPA, CA • Ted Baskerville, CA • Alan Brill, CISSP

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

The CPA's Handbook of Fraud and Commercial Crime Prevention

AICPA

Tedd Avey, CPA, CA • Ted Baskerville, CA • Alan Brill, CISSP

The CPA's Handbook of Fraud and Commercial Crime Prevention

Tedd Avey, CPA, CA•IFA • Ted Baskerville, CA•IFA • Alan Brill, CISSP

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

Kroll

The Risk Consulting Company

FORENSIC ACCOUNTING, LITIGATION CONSULTING BUSINESS VALUATION

NOTICE TO READERS

The CPA's Handbook of Fraud and Commercial Crime Prevention does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the authors and publisher are not rendering legal, accounting or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

First edition published March 2000. First revision April 2001.

1 2 3 4 5 6 7 8 9 0 PP 0 9 8 7 6 5 4 3 2 1

ISBN 0-87051-292-7

TABLE OF CONTENTS

PREFACE

"The Lord said to Moses... you shall not defraud or rob your neighbor." —Leviticus 19:1,13

"Where large sums of money are involved, it is advisable to trust nobody." —Agatha Christie

Fraud is estimated to cost the North American economy more than $400 billion annually, according to the Association of Certified Fraud Examiners. This figure may even be conservative when it is considered that insurance fraud alone costs U.S. industry $120 billion annually, as reported by Conning & Company, a prominent research and investment firm.

Despite these loud numbers, fraud is primarily a silent problem. Fraud experts estimate that more than 75 percent of frauds are undetected, and many that are detected are not reported. Firms do not disclose their losses resulting from fraud for many reasons, including that they are embarrassed that they have been defrauded, or they want to keep the bad news from clients and customers.

Perhaps because fraud is so underreported, many companies think it will never happen to them. Unfortunately, a firm unwilling to consider that its personnel, agents or vendors could act dishonestly is a fraudster's dream. What better environment to exploit than one in which the guard is down?

The purpose of this Handbook is to provide CPAs with practical information and resources to help them identify and respond to fraud in the workplace, with an emphasis on prevention rather than investigation. Although it is impossible to eliminate the risk of fraud completely, effective prevention policies can reduce opportunities for fraud to occur. At the same time, sophisticated detection methods can help uncover fraud in the early stages, minimize losses, and enable those affected by fraud, particularly CPAs or financial managers responsible for fraud prevention, to react to fraud in a way that could solve or mitigate the problem rather than contributing to it.

HANDBOOK OVERVIEW

The primary focus of this Handbook is fraud prevention. Since prevention cannot be realized without understanding how fraud is perpetrated and concealed, the material in this Handbook has been written to explain to CPAs the nature and extent of fraud and to familiarize them with general fraud prevention techniques. In addition to the core topics of fraud prevention and methods of combating specific kinds of fraud, two chapters are devoted to computer security and the unique kinds of crimes and criminals related to computer crimes.

The contents of the Handbook are summarized below, in brief synopses of each chapter, to provide readers an overview of the material.

CHAPTER CONTENTS

Managing the Risk of Fraud

Chapter 1, "Managing the Risk of Fraud," describes the concept of fraud risk: understanding it and guarding against the threat posed by it. The specific factors that affect fraud risk are addressed, including the key internal controls—basic, supervisory and audit—that help prevent fraud. Since detecting and preventing fraud in books of account is key to any prevention strategy, there is a section devoted exclusively to this topic, with fraud and AICPA Statement on Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit (AICPA, Professional Standards*, vol. 1, AU sec. 316) discussed in relation to fraud auditing. A comprehensive and practical risk management checklist is included at the end of the chapter.

Promoting an Ethical Environment

Because an ethical environment is a key element in any effective prevention strategy, chapter 2, "Promoting an Ethical Environment," describes the various steps that can be taken to promote an ethical environment within an organization, and thereby reduce the risk of fraud. A sample code of ethics and business conduct, which can be reproduced and/or adapted for use in any organization, is included, along with an ethical environment checklist.

Risk Financing and Fidelity Insurance

Risk management is a key component of fraud awareness and is essential for providing protection against potentially catastrophic risks, including fraud-related losses. Chapter 3, "Risk Financing and Fidelity Insurance," examines the concept of risk financing. The chapter gives a description of the kinds of fidelity insurance policies that are available—including some of the more typical policy clauses and the insured's responsibilities—and the factors that enter into the fidelity insurance purchase decision. A practical checklist is included at the end of the chapter.

Computer Security and System Recovery

Adequate computer security is an indispensable fraud prevention tool. Chapter 4, "Computer Security and System Recovery," provides a comprehensive overview of computer security, including physical security, logical security, and system recovery. A checklist is also included with this chapter.

Internal Fraud

Chapter 5, "Internal Fraud," addresses the various ways fraud is committed against an organization by a perpetrator from within that organization, meaning, by officers, managers, or employees—the most common form of fraud. Frauds are classified according to the various accounting cycles to which they relate: sales and collection, acquisition and payment, payroll and personnel, inventory and warehousing, and capital acquisition and repayment. Since cash is the focal point of most entities, a separate section is devoted to cash misappropriation.

External Fraud for Personal Gain

Fraud can also be committed against organizations by suppliers, professional con artists and other outside perpetrators. Chapter 6, "External Fraud for Personal Gain," is a discussion of the various ways frauds are committed against small businesses and individuals, the government, and financial institutions, such as banks and insurance companies. Case studies are included to clarify the various kinds of fraud perpetrated by outsiders.

Commercial Crime

In addition to being victimized by fraud, organizations can also be the perpetrators of fraud. Chapter 7, "Commercial Crime," provides an overview of the various forms of commercial crime and methods of preventing them. The crimes considered include false advertising, industrial espionage and trade secret theft, insider trading, securities fraud, organizational bribe giving. Interesting and informative case studies are included to exemplify the different kinds of commercial crime.

Computer Crime and Computer Criminals

Although it has resulted in very few genuinely "new" frauds, the computer has dramatically changed the environment in which fraud is committed. Chapter 8, "Computer Crime and Computer Criminals," is a description of the nature of computer-related crime and computer criminals and the control considerations that affect the risk of fraud in a computer environment, and provides selected computer crime case studies.

Addressing a Known or Suspected Fraud

Despite the best prevention strategies, an actual crisis may strike. Chapter 9, "Dealing With a Known or Suspected Fraud," focuses on crisis management and, more particularly, forensic accounting. A comprehensive checklist is included at the end of the chapter.

Reducing the Risk of Financial Statement Fraud

Financial statement fraud is of prime importance to CPAs because of their direct involvement in creating or reviewing financial statements, whether as an employee of a company or as a company's independent auditor. Chapter 10 focuses on the nature of financial statement fraud, the motivations for these frauds, the qualitative and quantitative predictors of these frauds, and special areas to consider. A comprehensive checklist is included at the end of the chapter.

APPENDICES

A—Fraud Sector-By-Sector

This comprehensive section outlines a breakdown of fraud in the different sectors, complete with checklists and fraud vulnerability grids for each of the following sectors:

- Construction
- Financial services
- Government
- High technology

- Manufacturing
- Media and communications
- Nonprofit
- Professional services
- Real estate
- Recreation
- Natural resources
- Retail
- Small business
- Transportation
- Wholesale

B—Statement on Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit*

A complete text version of SAS 82 is provided as Appendix B for reference.

Bibliography

This alphabetical listing of the most current and relevant sources of information, including a separate section for Web sites and books, pertaining to fraud, commercial crime, and other closely related topics for further reading.

Glossary

The comprehensive glossary is an effective quick-reference tool which provides an alphabetically arranged listing of definitions and explanations for all fraud-related terms and kinds of fraud.

ACKNOWLEDGMENTS

The CPA's Handbook of Fraud and Commercial Crime Prevention is the result of considerable effort on the part of many individuals. The authors would especially like to thank Paul Dopp, Jim Murray, Ian Ratner, Pat Woytek, Kip Hamilton, Kevin Brant, Todd Horn, Dave Iverson, Tae Kim, Ron Gelinas, Angela Fernandes, and all the others at Kroll Lindquist Avey for their assistance.

A special thanks to Patricia M. Adamson, BA, MISt, who painstakingly edited the final drafts of the Handbook, making it more readable and consistent. We would also like to acknowledge the Canadian Institute of Chartered Accountants and in particular, Peter Hoult, who was responsible for overseeing the development and publication of *The Accountant's Handbook of Fraud and Commercial Crime,* which forms the basis of this Handbook.

We are grateful to a long list of other individuals and companies who assisted in this version of the Handbook, including Joe Wells and the Association of Certified Fraud Examiners.

ABOUT THE AUTHORS

Tedd Avey, BComm, CPA, CA•IFA, CFE, is the worldwide head of the Financial Services Group of Kroll, The Risk Consulting Company and President of Kroll Lindquist Avey in Toronto. Kroll Lindquist Avey is an international professional service firm specializing in fraud investigation, business valuation, commercial litigation, insurance claims, and due diligence services. Tedd's practice is focused primarily on complex and large-scale corporate investigations and commercial litigation throughout the United States, Canada, Europe, and the Middle East, and includes cases ranging from several million to hundreds of millions of dollars. Tedd has twenty-five years' experience in forensic and investigative accounting and has written numerous articles and books on the subject, including coauthoring *The Accountant's Handbook of Fraud and Commercial Crime*, a publication of The Canadian Institute of Chartered Accountants. Tedd is an accomplished speaker and seminar leader on fraud prevention and detection to accountants and law enforcement personnel throughout North America and in other major cities around the world.

Ted Baskerville, BA, CA•IFA, CFE, is head of the Forensic Accounting Practice of Kroll Lindquist Avey in the United Kingdom. Ted has more than twenty years' experience in forensic accounting. Ted's extensive experience in the insurance claims industry includes assessing the basis for and quantum of claims for fidelity and property losses, and business interruption matters. His areas of expertise include corporate investigations and civil litigation matters covering issues of loss of income, partnership and shareholder disputes, breach of contract, breach of fiduciary duty, insurance claims for property and employee fidelity, and civil fraud. Ted has participated in numerous major investigations involving employee dishonesty, secret commissions, and other forms of management and employee corruption. Ted has presented seminars on fraud awareness, insurance claims, and investigative accounting techniques to the insurance and financial services industries, the legal and corporate communities, law enforcement personnel, members of government ministries, accounting groups, and other professional associations.

Alan Brill, BA, MBA, DPS (ABD), CISSP, is Senior Managing Director heading up the High Tech Investigations and Computer Forensic Group worldwide of Kroll Associates in New York. Alan has an international reputation in the areas of computer/communication security and technology crime investigation. His work has ranged from major information security reviews for multi-billion dollar corporations, to criminal investigations of computer hackers; telephone phreakers; and PBX cellular, E-Mail, and Voice Mail frauds. Alan is a frequent speaker at conferences and has been featured in both print and broadcast media. Alan has authored books and articles and has been called as an expert witness in numerous computer forensic cases.

William (Bill) L. Jennings, BS, CPA, CFE, is a Principal of Kroll Lindquist Avey in Chicago and head of the Financial Services Group for the Midwest Region. Bill has more than twenty years' experience in fraud investigation, forensic accounting, public accounting, and auditing. His casework includes multi-million dollar fraud investigations, healthcare fraud, commodities fraud, criminal tax fraud, embezzlement, securities fraud, money laundering, purchasing fraud, bank fraud, theft by conversion, and public corruption. Bill has assisted with the development and implementation of new or enhanced compliance programs and compliance audits both in the healthcare industry and for government contractors. Bill has written articles on many of these topics, given numerous presentations, and is a highly respected expert witness.

Charles Lundelius, Jr., CPA, ABV, BS, MBA, is a Principal and head of the U.S. Securities Litigation Services Group of Kroll Lindquist Avey in Washington, D.C. His twenty years in the accounting field have included seven years in securities and investment banking and more than eight years in consulting and litigation services. Charles currently specializes in the valuation of securities and intellectual property. He has consulted and/or testified in the areas of securities market pricing, investment suitability, securities fraud, compliance and due diligence practices. He has qualified as an expert in securities trading and valuations, damages, financial analysis, accounting, statistics and econometrics. An experienced public speaker, Charles has presented at professional seminars and conferences on a variety of accounting and legal topics.

Daniel (Dan) W. Ray, CPA, CFE, CIRA, is a Director in the Litigation Services Group in the San Francisco office of Hemming Morse, Inc. As a CPA and former Special Agent for the FBI, Dan has concentrated on forensic accounting, fraud investigation, and bankruptcy-related cases for more than eighteen years of his professional career. His combined expertise in accounting and fraud investigations has enabled Dan to assist attorneys in the areas of document discovery, analysis of business and accounting records, deposition assistance, and development of trial exhibits. As a CPA, Dan has worked as a consultant and expert witness in civil and criminal cases and has assisted both prosecution and defense, testifying in federal, state, and local courts.

Hazel de Burgh, BMath, CA•IFA, CFE, is a Principal of Kroll Lindquist Avey in Toronto. Hazel has worked exclusively in the area of forensic and investigative accounting since 1986, with a focus on commercial litigation matters and corporate investigations, many of which have involved multi-million dollar cases. Hazel's areas of expertise include procurement fraud investigations, asset tracing assignments, and the assessment of financial issues in complex commercial litigation. She has coauthored a manual on procurement fraud, and led numerous presentations on these and other related topics to internal audit professionals, corporate executives, lawyers, and law enforcement personnel. She has written articles for various trade publications.

Paul Dopp, CPA, CGA, CFE, of Kroll Lindquist Avey, Atlanta, has twenty years' experience in forensic and investigative accounting, corporate investigations, litigation support and due diligence services, with his case experience including civil, criminal and regulatory matters. Paul has given presentations to professional organizations and law enforcement personnel regarding the investigative issues of fraud and white collar crime and has written articles on forensic accounting-related topics, including procurement fraud and electronic fraud.

Ian Ratner, CPA, CA, CBV, ASA, CFE is currently the CFO of TIC Enterprises, Atlanta, a leading sales outsourcing firm primarily focused on the telecommunications industry. Ian's areas of expertise include public and forensic accounting, damage calculations, and business valuation services. Ian is primarily responsible for marketing and execution of various forensic accounting and litigation support cases. His case experience includes civil, criminal, and regulatory matters, specializing in business valuations, economic damage assessments in business disputes and intellectual property matters, financial investigations, pre- and post-due diligence analysis and investigations, bankruptcy, money laundering, and internal corporate investigations.

Howard Silverstone, FCA, CFE, has concentrated on forensic and investigative accounting since 1985, and has experience as a financial investigator and auditor on hundreds of forensic accounting and claims assignments both in North America and internationally. As a Principal in the Philadelphia office of Kroll Lindquist Avey, Howard has been involved in every aspect of cases, including planning, detailed analysis, assistance with all phases of discovery, and expert testimony at deposition and trial in connection with loss assessment, fraud, and related financial issues. His cases include economic damages, fraud investigations, fidelity bond analysis and surety matters, among many others. A native of the United Kingdom, Howard is a member of the Pennsylvania Institute of Certified Public Accountants.

Patricia Woytek, BA, MIS, CPA, specializes in forensic and investigative accounting at Kroll Lindquist Avey, Philadelphia. For almost twenty years, Pat has specialized in complex financial and forensic analyses of financial statements, tax returns, accounting records, contracts, and agreements. Her casework includes fidelity and surety losses, directors and officers negligence, business income losses, lost profits and economic damages, commercial damage calculations, corporate fraud investigations, damages in breach of contract disputes, and damages caused by financial institution failures. Pat has also written for *The Risk Report*, published by the International Risk Management Institute and has given numerous speeches on the subject of fraud.

Charmaine Raphael, BBA, MBA, MS, CFE, of Kroll Lindquist Avey, New York, has specialized in computer systems and data analysis in fraud investigations and corporate litigation for more than eleven years. She has worked with various law enforcement agencies both in New York on organized crime investigations involving the New York City Transit, and in London on fraud investigations with the City of London Fraud division and the Serious Fraud Office. Charmaine also worked in Germany on behalf of the London Postal Office reviewing a 12-million Sterling contract with a major German technology company. Charmaine has developed and presented courses on the use of technology in investigations to accountants, investigators, and law enforcement personnel in New York and London.

David M. Shapiro, CPA, MBA, JD, BA, is a Director of the Financial Services Group for the New York office of Kroll Lindquist Avey. David has combined his legal and accounting backgrounds to concentrate on forensic accounting and litigation support since 1993. In addition, he has eight years' prior experience in the investigation and prosecution of frauds and related criminal conduct as a Special Agent for the FBI in New York, and Assistant Prosecutor in New Jersey. David's casework includes criminal prosecutions and civil litigation involving businesses and professional practices. He has testified in depositions of matters in federal and state courts arising from dissident shareholder actions. David has presented training seminars on litigation support and compliance programs.

CHAPTER 1:

Managing the Risk of Fraud

CHAPTER 1:

Managing the Risk of Fraud

1.1 THE NATURE AND EXTENT OF FRAUD

1.1.1 Definitions

The key word used in most dictionaries to define fraud is *deception.* In the broadest sense of the word *fraud,* this definition may be sufficient. However, in the context of this Handbook, a slightly more restrictive definition is appropriate: fraud is *criminal deception intended to financially benefit the deceiver.* Both of the qualifiers in this definition are necessary—that is, the deception must be *criminal* in nature and involve *financial benefit.*

Criminal Deception

The qualifier *criminal* is necessary to exclude certain deceptions that may financially benefit the deceiver—for example, the mild overstatement of one's skills on a job application; however, this kind of transgression will not be examined in this Handbook. While such an overstatement could be labeled *fraudulent* in the broadest sense of the word, it can hardly be described as criminal.

Note that, for purposes of this definition, the word *criminal* is not used in a strict legal sense. Rather, it refers to a seriously "wrong" action taken with malicious intent. Thus, even if perpetrators of fraud are able to avoid successful criminal prosecution—for example, because a particular jurisdiction has lax laws or enforcement, or because of some legal technicality—their actions are still considered "criminal" for purposes of this Handbook.

Financial Benefit

The qualifier *financial benefit* is necessary in order to exclude certain types of criminal deception that we do not commonly think of as fraud and therefore, are not dealt with in this Handbook—for example, a wealthy bigamist failing to disclose a previous marriage.

The financial benefit accruing to the fraudster from an action need not be direct for that action to be considered fraudulent. Indirect financial benefits are also possible, for example, environmental criminals (fraudsters) who dump toxic waste into rivers to avoid higher disposal costs and falsify records to conceal their actions.

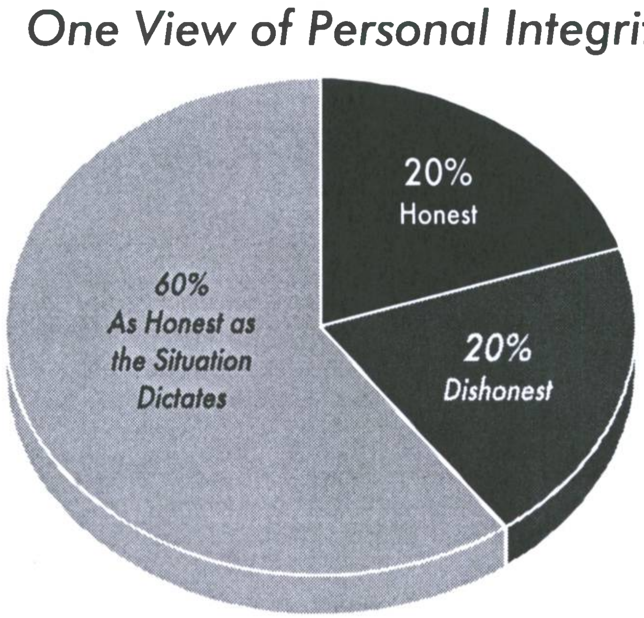
1.1.2 Magnitude of the Threat

Because the essence of fraud is deception, determining its prevalence is problematic. Many frauds go undetected—probably more than 75 percent—and many frauds that are detected are not reported. It is virtually impossible to compile reliable statistics under these circumstances.

Simply based on the largest reported frauds—for example, the U.S. savings and loan scandal, BCCI, Boesky and Milken—it is safe to say that fraud in the United States runs in the billions of dollars. If one assumes that fraud represents about 3 percent of gross national product (GNP)—conservative by some estimates—then the total cost in the United States would be about $300 billion.

Macro statistics are not particularly meaningful, however, even if you could obtain accurate statistics. The fact is that the threat of fraud depends largely on the circumstances, that is, the environment in which it takes place. Let's begin with a view of personal integrity, as illustrated by Figure 1-1.

Figure 1-1. One View of Personal Integrity



Views of commitment to personal integrity vary, and the percentage figures shown are not definitive. Some views suggest a more even split between the three categories, while others state that the honest and dishonest categories may be as low as ten percent each. However, all of these views point to one important conclusion: exclusive reliance on the honesty of individuals is the surest way to be victimized. Over half the population—and probably more than two thirds—is quite capable of committing dishonest acts in the right (or should we say wrong?) environment.

The importance of creating an environment that discourages fraud brings us back to the question "What is the magnitude of the threat?" Answer: *the threat of fraud is as big as it is allowed to be.*

1.1.3 Sources of the Threat

The magnitude of the fraud threat is only one dimension contributing to the extent of the problem. The breadth of the fraud threat—that is, the various sources of fraud—must also be considered. A truly comprehensive prevention strategy must address the full spectrum of fraud sources.

You can classify the sources of the fraud threat as either internal or external collusion. A brief description of each classification follows.

Internal Sources

Internal opportunities to commit fraud differ from company to company. Some typical examples, which illustrate the broad nature of these internal opportunities, include the following.

- Officers of a company create false financial reports to improve their own performance measurement.
- Managers inflate their expense accounts or turn a blind eye to supplier fraud in exchange for kickbacks.
- Other employees commit fraud such as embezzlement, cash skimming, or accounts receivable lapping.
- Corporate directors defraud a company's shareholders through stock market manipulation or insider trading.

External Sources

Typical examples of external opportunities to commit fraud include the following.

- Suppliers falsify or duplicate invoices.
- Competitors victimize a company through industrial espionage or price fixing.
- Con artists defraud a company with schemes involving products, services, or investment opportunities that never materialize.
- Customers commit fraud through false credits posted to their accounts or through rebate coupon frauds.

See figure 1-2 for a depiction of the various internal and external sources of fraud.

1.1.4 The Causes of White Collar Crime

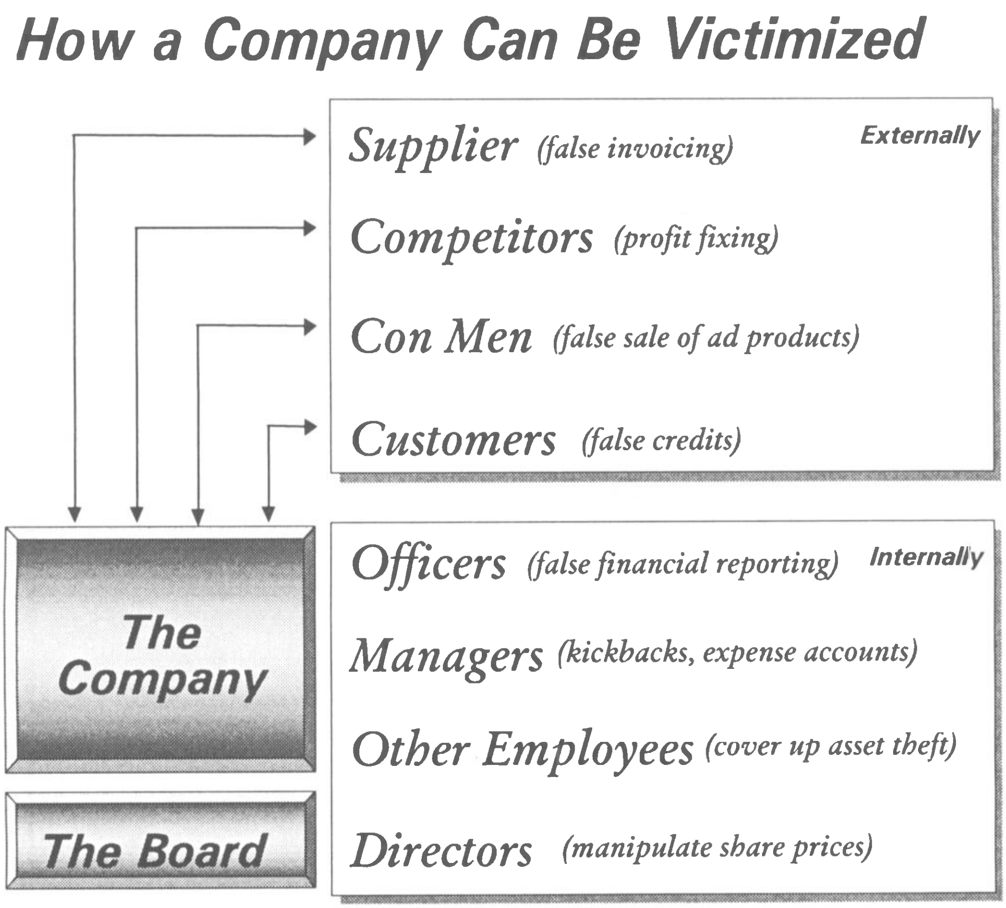
The theory of *differential association* is undoubtedly the best known among all explanations offered to account for crime. Although it applies to all forms of crime—not just white collar crime—it is nevertheless useful for the purposes of this Handbook.

This theory first appeared in 1939 in the third edition of Edwin H. Sutherland's *Principles of Criminology*. Later, Sutherland would make his best-known contribution to criminology by coining the phrase *white-collar crime* and writing a monograph on the subject.

Based on nine concepts or *points*, the theory of differential association begins by asserting that criminal behavior is learned. Expanding on that assertion, Sutherland specifies as a second point that criminal behavior is learned in interaction with other people in a process of communication. If individuals acquiring criminal habits or propensities were exposed to situations, circumstances, and interactions totally of a criminal nature, it would be relatively easy to comprehend how this process of communication operates. In view of the enormous variation in standards and personalities to which any individual in our society is exposed, it becomes exceedingly difficult to discern the elements that induce criminal behavior without some additional principles.

Sutherland's third point is that criminal behavior is acquired through participation within intimate personal groups. This suggests that the roots of crime are in the socializing experiences of the individual. Unfortunately, the process of socialization is far from adequately understood. Sutherland's fourth point indicates that the criminal learning

Figure 1-2. How a Company Can Be Victimized



process includes not only techniques of committing crime but also the shaping of motives, drives, rationalizations, and attitudes. Crime techniques often can involve a high degree of skill: picking pockets (and not getting caught at it) demands considerable adroitness.

Fifth, Sutherland stipulates that legal codes define the specific direction of motives and drives as favorable or unfavorable.

Sixth, Sutherland establishes the principle of *differential association.* According to this postulate, a person becomes criminal because of an excess of definitions favorable to violation of the law over definitions unfavorable to violation of the law. Sutherland states in his seventh point that differential association may vary in frequency, duration, priority, and intensity. But he does not suggest which of these elements is apt to be more important than the others.

Sutherland's eighth point is that learning criminal and delinquent behavior involves all the mechanisms that are involved in any other learning. As his next to last proposition Sutherland stresses that learning differs from pure imitation.

The last point is a worthwhile reminder that while criminal behavior is an expression of general needs and values, it is not explained by these general needs and values because noncriminal behavior is an expression of the same needs and values. This means that the generalizations sometimes employed to account for crime—that people steal because they crave "esteem" or are "greedy" or kill because they are "unhappy"—have little scientific merit.

In other words, much of the same needs and values motivate criminals and noncriminals alike. People become or do not become criminals on the basis of their unique responses to common drives for prestige, happiness, success, power, wealth, and other human aspirations. One person with a pressing need for money may take an extra weekend job pumping gas, or try to borrow from a friend. Another person, feeling the same need, may hold up a fast food outlet.

1.1.5 Understanding the Risk

Of the two available ways to combat fraud—prevention and detection—a prevention strategy is obviously the preferred approach. Such a strategy can be either general or specific in its objective. General prevention techniques for risk management involve two main elements: understanding the risk and guarding against the threat.

Fraud Versus Theft

Resolved: fraud is not the same as theft.

In a debate, most people would choose to defend the above statement. They might win by arguing that—

- Theft is like robbing a bank; fraud is like cooking the books to cover up petty cash theft.
- People committing theft do so at night, wearing masks; people committing fraud do so during the day, wearing suits.
- Theft is direct; fraud is indirect.
- Theft is what lower-class criminals commit; fraud is what upper-class criminals commit.

Few people, if any, however, will point out what is perhaps the most important difference between fraud and theft: the risk of fraud is much greater.

With an increasingly high media profile given to crime, particularly in large cities, most people are acutely aware of the need to protect themselves against crime's overt forms. In a bad neighborhood, for example, you would not leave the keys in your car or the doors unlocked. In fact you probably would not want to be there at all. In this case the risk of theft, a more overt and direct form of criminal act than fraud, is easy to assess and deal with.

Now consider a different scenario: if you were to leave your wallet briefly on your desk at work, you would also be exposing yourself to a risk. However, assuming that access to your workplace is restricted to other employees, in all likelihood, you would consider this risk to be a very small one. Presumably the people you work with aren't criminals and would never pick up your wallet in a direct act of theft. The risk of being detected, as perceived by a perpetrator, would be relatively high. You would certainly know that your wallet had been stolen and a thorough investigation would ensue, possibly implicating a coworker.

Herein lies the first of two pillars on which the greater threat of fraud is built. One pillar is based on the premise that most people believe that those who are relatively close to them—their friends and coworkers—are basically honest. Potential victims may rationalize about those around them: "They would never steal. As long as we lock the doors at night to keep out the 'real crooks,' we'll be safe."

The other pillar is based on the perception that fraud is in some sense an indirect form of theft. Although a criminal act, people who perpetrate fraud will in many cases rationalize their behavior, believing that because it's indirect, it's victimless. Alternatively, the perpetrator may rationalize that the victim deserves it, or where the amount involved in the fraud is low in relation to the total assets available, that the victim can afford it and—or won't—even miss it. And so the second pillar is formed from the rationalizations of most fraudsters—the denial that the fraud is morally wrong: "No one will be hurt by this. The company won't even miss it. Besides, they deserve it for the lousy way they treat me."

These two pillars—low perception of the threat of fraud by potential victims, and a high degree of rationalization by potential perpetrators—combine to make fraud a much more insidious threat than ordinary theft. A further illustration of this greater risk: according to a report in a 1999 FBI *Law Enforcement Bulletin*, check fraud in 1994 was estimated to have an impact on financial institutions, private business, and the public that ranged from $815 million up to $10 billion. Further, according to bank executives, check fraud is the major crime problem facing the financial community. The enormity of the fraud problem is illustrated by another FBI report that indicated that about $60 billion in mortgage loans processed annually involved some degree of fraud and that in 1996, 35 percent of the $3.3 billion of reported losses in the financial institution fraud criminal referrals the FBI received involved some type of loan fraud or false statement.

Generic Versus Individual Risk Factors

A large number of factors can impact the risk of fraud. This Handbook contains an approach—a system of categorization—that facilitates the understanding of fraud risk and the development of an appropriate strategy to manage it.

The literature is filled with many different systems of categorizing fraud risk. The system developed for this Handbook splits the risk factors into two groups: generic and individual.

Generic risk factors remain relatively constant in their impact on any subject individual or group of individuals. They are largely within the control of the organization or entity that is protecting itself, and largely outside the control of potential perpetrators. Because these risk factors apply in the same way to any employee, they can be set and manipulated by an organization without considering individual differences among employees. Employee turnover has virtually no effect on these risk factors.

Individual risk factors change from person to person and can even change for the same individual over time. They are only partially within the control of the organization or entity that is protecting itself, and this control is more difficult to exercise because it applies to each individual separately. Whenever turnover occurs, the individual risk factors change and must be managed. Even worse, whenever an individual's personality, state of mind, circumstance, or motivation changes—which, after all, is a constant process—the associated risk factors may also change.

See sections 1.2.1 and 1.2.2 for a more detailed discussion of generic and individual risk factors.

1.1.6 Guarding Against the Threat

On understanding the risk of fraud, you must develop an appropriate strategy and implement policies to guard against the threat. The main elements of this process are:

- Choosing acceptable risk levels
- Developing and implementing internal controls
- Promoting an ethical environment
- Arranging appropriate risk financing (insurance)
- Ensuring adequate computer security

Choosing Acceptable Risk Levels

The risk of fraud can never be completely eliminated. Even if this were possible, it would probably not be desirable because of prohibitive costs and extremely tight controls that would stifle creativity and make employee morale suffer. The first step in a fraud-prevention strategy is to determine the acceptable level of risk.

Choosing acceptable risk levels intertwines with assessing the various risk factors. For example, one of the generic risk factors is the *opportunity risk* available to potential perpetrators. Assessing this opportunity risk enables you to make other decisions—such as: "Do we need to lower this risk, and if so, by how much?"

Developing and Implementing Internal Controls

Internal controls—consisting of basic controls, supervisory controls, and audit—represent the cornerstone of any fraud prevention strategy.

To ensure complete and accurate reporting an internal control system must be designed and implemented *regardless* of the risk of fraud. However, a system should never *disregard* the risk of fraud; such disregard would amount to a virtual invitation to potential perpetrators.

See section 1.3 for a detailed discussion of internal controls.

Promoting an Ethical Environment

Promoting an ethical environment is another key element in a prevention strategy. In particular implementing a formal code of ethics and business conduct helps set the tone for all employees within an organization. See chapter 2 for further discussion.

Arranging Appropriate Insurance

Recognizing that there will always be some risk of fraud, organizations must finance this risk either externally and explicitly (fidelity insurance) or internally and implicitly (self-insurance). See chapter 3 for further discussion.

Ensuring Adequate Computer Security

Computers and information technology play an increasingly important role in business and society in general. The pervasive nature of these technologies demands that adequate computer security be an integral part of any prevention strategy. Although computer security may be considered a subset of internal control, it is still an important aspect. See chapter 4 for details.

1.2 FRAUD RISK FACTORS

Several factors contribute to the risk of fraud. Organizations use various systems for categorizing these factors; however, under most systems, the elements that combine to determine fraud risk are largely the same.

For example, one classification system is known as the GONE theory, an acronym for *Greed, Opportunity, Need,* and *Exposure.* Under this system, the Greed and Need factors relate largely to the individual (that is, the potential perpetrator), while the Opportunity and Exposure factors relate largely to the organization (that is, the potential victim). The four elements of the GONE theory interact to determine the level of fraud risk, and no one factor is universally more important than another. Each of the factors is unfavorable, to some extent, in virtually all situations. However, an organization that allows a sufficiently unfavorable or an out-of-balance combination of all four factors may face serious troubles. As one fraud investigator observed, "You can consider your money GONE."

In this Handbook we use a slightly different system that groups the risk factors into generic or individual, as previously defined. However, as described below, many of the same elements of the GONE theory apply under this system as well.

1.2.1 Generic Risk Factors

Generic risk factors—those largely under the control of the organization or entity that is protecting itself—include:

- The opportunity given to potential perpetrators.
- The likelihood of discovering a fraud that was committed.
- The nature and extent of the punishment a perpetrator will receive once the fraud is uncovered and the perpetrator is caught.

Note that the first factor corresponds to the "O" or Opportunity in the GONE theory, while the second and third factors correspond to the "E" or Exposure risk element. The Exposure risk under the GONE theory is a product of two generic factors: the likelihood of getting caught and the subsequent consequences. The product of both must be low for there to be any risk to the organization. For example, if the likelihood of getting caught is 0 percent, then the exposure risk is 100 percent. Similarly, if the consequences of getting caught are insignificant, then the exposure risk is high.

A brief description of each generic risk factor follows.

Opportunity to Commit Fraud

The opportunity to commit fraud refers primarily to allowing a potential perpetrator access to the assets of the organization or object of the fraud. No organization can completely eliminate opportunity; experts consider such attempts uneconomical and counterproductive. As long as organizations have assets of value and these assets flow, are traded or come under the control of others—such as employees, customers and suppliers—the opportunity to commit fraud will always exist.

For organizations the challenge in fraud prevention is ensuring that the opportunity risk level is minimal under the circumstances, that is:

1. Assign, either explicitly or implicitly, to each employee an appropriate maximum opportunity level. For example, limit a junior clerk's opportunity level to certain smaller fixed assets not bolted down in the office. Allow a more senior clerk's maximum opportunity level to include an additional $500 petty cash fund, or the day's cash receipts. Allow a senior executive an additional $5,000 check-signing limit.
2. Prohibit catastrophic opportunity levels. The definition of a catastrophic level depends on the circumstances—in particular, the size of the organization. For example, a small business with $50,000 in cash should probably not allow anyone but its owner(s) access to the full amount.

Likelihood of Discovery

If an opportunity to commit fraud exists, making the chances of discovery high reduces the risk. In fact, even the *perception* that the chances of discovery are high can act as a deterrent. Of course, if a fraud does occur, *discovery* may result in *recovery* of some of the lost assets.

The likelihood of discovery stems primarily from the system of internal controls. While these controls can never be so tight as to preclude any fraud from taking place, ideally they should be sufficient to prevent most material frauds from going undetected for any length of time.

Another factor that could increase the chance of discovery is encouraging employees to take an active role in reporting suspected fraud activities. Publicizing the impact of fraud on employer profitability and fraud's negative effect on employee profit-sharing benefits has worked to stimulate employee efforts to curtail fraud.

See section 1.3 for a closer look at internal controls.

Nature and Extent of Punishment

Discovery of a fraud is, in itself, insufficient to act as a deterrent against future fraud. Organizations must put in place some adverse consequences for potential perpetrators, who, most important, must perceive these adverse consequences.

Although research has not provided proof, conventional wisdom holds that the nature and extent of punishment has a deterrent impact. The occurrence of theft in countries governed by Islamic law is extremely low compared to Western countries. Presumably this is due, at least in part, to the severity of the punishment (amputation of one or both of the hands). Can anyone doubt that the occurrence of theft in North America would diminish if perpetrators knew they would face the same punishment? Of course, the reality is that the punishment must "fit the crime" and be consistent with a society's justice system.

Organizations or entities wishing to protect themselves from fraud should have clear policies regarding the nature and extent of the consequences of getting caught; for example—

- Anyone who commits a fraud will be dismissed.
- All frauds will be reported to the authorities and charges will be laid.

1.2.2 Individual Risk Factors

Individual risk factors—those that vary from employee to employee, largely outside the control of the organization or entity that is protecting itself—fall into two categories:

1. Moral character
2. Motivation

Moral character corresponds to the "G" or Greed factor in the GONE theory, while motivation is equivalent to the "N" or Need factor. Each of these categories is described below.

Moral Character (Greed Factor)

Greed represents broad concepts, such as ethics and moral character, or the lack thereof. Moreover *greed* and *ethics* essentially relate to the internal or personality attributes of an individual, as do *character, integrity, honesty,* and the like. You cannot know whether an individual possesses these attributes without the ability to read that individual's mind. Even if this were possible, personal interpretation would still come into play.

Social values also have an impact on moral character. Many sociologists lamented a trend in Western societies during the 1980s, namely the pursuit of wealth as an overriding objective. The *Me Generation* and the *Decade Of Greed* were phrases coined in connection with this trend, which was perhaps best epitomized by the memorable speech of Michael Douglas' Gordon Gecco character in the 1987 movie, *Wall Street:* "Greed is right. Greed is good. . ."

In fact, Gordon Gecco's philosophy may hold some element of truth. A certain amount of greed, tough-mindedness, and competitive instinct could greatly enhance the chances of success for an organization or an individual in a free enterprise society. Regardless of one's own value judgment, there is no doubt that these attributes do exist in society. This poses a problem, however, because, while greed may not necessarily preclude the existence of ethics and good moral character, if left unchecked or promoted to a great extent, it can have an adverse impact *vis-à-vis* the risk of fraud.

This leads to the essential question at issue here: What can or should an organization do to minimize the risk of fraud posed by greed and other negative human attributes? Consider the following.

- *Corporate Mission Statement:* Set the goals of an organization in a corporate mission statement, and communicate it to all managers and other employees. The primary goal of most businesses is to maximize profits, presumably over the long-term in order to survive. Other objectives might include maintaining either a high market share, leadership in an industry, or both. However, businesses must pursue these goals in a manner consistent with good corporate citizenship and standing in the community. This emphasis on corporate responsibility sets the tone for management and employees, and encourages personal responsibility. Conversely, business should discourage irresponsible actions—and by extension, fraud.
- *Written Codes of Business Conduct:* "Good moral character" means different things to different people; an organization must define this term and relate it to particular types of behavior. For example, does your organization consider it moral and ethical for its employees to accept gifts from customers and, if so, is there a specified value or limit? A written code of ethics and business conduct can help translate the relative concepts of greed, ethics, and morality into more specific behaviors that are either acceptable or unacceptable.
- *Management Style and Role Models:* Management must set the right example for employees by acting responsibly and living up to the spirit of the corporate mission statement and code of business conduct. Moreover, it must clearly and visibly appear to do so in its dealings and communications with employees. Policy statements mean nothing when undermined by management's actions. In fact, such a situation may be worse than having no policy at all because management's failure to adhere to its own guidelines would foster a kind of cynicism and "rules are made to be broken" philosophy that might potentially encourage fraud and commercial crime.
- *Hiring Practices:* Regardless of corporate mission statements, codes of business conduct, and good role models, moral character ultimately depends on the individual employee. To the extent possible set hiring practices that weed out prospects with low moral character. See chapter 3 for further discussion.

Motivation (Need Factor)

Why do people commit fraud? There is obviously no single, specific answer. People commit frauds for a variety of reasons.

Probably the most common group of fraud motivations relates to economic need. For example, the perpetrator may be experiencing an actual or perceived cash emergency: a mortgage to pay, drugs to purchase to satisfy an addiction, or gambling losses to win back. Alternatively, there may be no emergency but simply an unchecked desire for the good life: expensive restaurants, clothes, furs, jewelry, vacations, cars, homes, and summer cottages.

Less frequently, there might be other reasons, such as, disenchantment, revenge, or simply the fact that everyone else seems to do it. Even more rarely, the motives could be eccentric: a sense of challenge or thrill. Finally, the cause may be some form of psychological illness: compulsion, anxiety, paranoia, or outright psychosis.

What can be done about all of these complex motives, seemingly locked up in the Pandora's box of an employee's mind? Admittedly, the options are limited but they include—

- *A Favorable Environment:* Creating the right environment can reduce the motivation among employees to commit fraud. In an unfavorable environment, morale suffers and feelings of disenchantment—even hate and the desire for revenge—may take hold. Try to promote the right environment by treating employees fairly, keeping communication lines open, and providing mechanisms for discussing and resolving grievances.
- *Performance Appraisal and Reward Systems:* Measure each employee's work fairly by implementing a performance appraisal and reward system.
- *Employee Assistance Programs:* Many enlightened employers provide free counseling and other assistance to employees facing personal problems, for example, alcohol and drug abuse. From the point of view of fraud prevention, this approach is preferable to keeping these problems "bottled up." This approach helps prevent resentment that could ultimately lead to the commission of fraud.
- *Employee Testing and Screening:* As part of their hiring practices and sometimes on a regular basis thereafter, some employers use testing and screening procedures to identify and weed out high risk individuals, or form the basis for remedial action, or both. Procedures include psychological testing, drug testing, and even honesty testing in the form of lie detector tests where not prohibited by law. Highly controversial, these tests, in some instances, could cause more harm than good, for example, to employee morale, the organization's reputation among prospective employees, and so on. Nevertheless, in especially sensitive occupations or circumstances, employers might find this testing appropriate and even necessary.
- *Common Sense and a Watchful Eye:* While motives are not observable, the product of certain motives often is. An employee with a drug or gambling problem may not be able to keep it a secret. And beware the $25,000-a-year bookkeeper who comes to work driving a Mercedes or who, wary of getting caught, never takes a vacation.

Profiles of Fraud Perpetrators

While external pressures do play a major role in whether or not an individual commits fraud, internal characteristics can affect a potential fraud perpetrator as well. Gwynn Nettler in his book, *Lying, Cheating and Stealing,* makes the following observations:

- People who have experienced failure are more likely to cheat.
- People who are disliked and who dislike themselves tend to be more deceitful.
- People who are impulsive, distractible, and unable to postpone gratification are more likely to engage in deceitful crimes.
- People who have a conscience (fear, apprehension, and punishment) are more resistant to the temptation to deceive.
- Intelligent people tend to be more honest than ignorant people.
- The easier it is to cheat and steal, the more people will do so.
- Individuals have different needs and therefore different levels at which they will be moved to lie, cheat, or steal.

- Lying, cheating, and stealing increase when people are under great pressure to achieve important objectives.
- The struggle to survive generates deceit.

The highly publicized cases in recent years of computer hackers committing high-tech crimes have resulted in a public perception that individuals who are highly knowledgeable about computers are more likely to commit fraud; however, there is no evidence to support this premise.

1.2.3 High Fraud-Low Fraud Environments

Employee fraud, theft, and embezzlement are more likely to occur in some organizations than others. The most vulnerable organizations are usually hampered by weak management and inadequate accounting and security controls. Solutions often proposed include:

- Tight accounting and audit controls
- Thorough screening of applicants for employment
- Close supervision and monitoring of employee performance and behavior
- Explicit rules against theft, fraud, embezzlement, sabotage, and information piracy

Other considerations also affect the likelihood of employee crime. See table 1.1 for a comparison of the environment and culture of organizations with high fraud potential and organizations with low fraud potential.

TABLE 1.1 ENVIRONMENTAL AND CULTURAL COMPARISON OF THOSE ORGANIZATIONS WITH HIGH FRAUD POTENTIAL AND THOSE WITH LOW FRAUD POTENTIAL.

Variable	High Fraud Potential	Low Fraud Potential
1. *Management style*	a. Autocratic	a. Participative
2. *Management orientation*	a. Low trust b. Power-driven	a. High trust b. Achievement-driven
3. *Distribution of authority*	a. Centralized, reserved by top management	a. Decentralized, dispersed to all levels, delegated
4. *Planning*	a. Centralized b. Short range	a. Decentralized b. Long range
5. *Performance*	a. Measured quantitatively and on a short term basis	a. Measured both quantitatively and qualitatively and on a long term basis
6. *Business focus*	a. Profit-focused	a. Customer-focused
7. *Management strategy*	a. Management by crisis	a. Management by objectives
8. *Reporting*	a. Reporting by routine	a. Reporting by exception

(continued)

TABLE 1.1 *(continued)*

Variable	High Fraud Potential	Low Fraud Potential
9. *Policies and rules*	a. Rigid and inflexible, strongly policed	a. Reasonable, fairly enforced
10. *Primary management concern*	a. Capital assets	a. Human, then capital and technological assets
11. *Reward system*	a. Punitive b. Penurious c. Politically administered	a. Generous b. Reinforcing c. Fairly administered
12. *Feedback on performance*	a. Critical b. Negative	a. Positive b. Stroking
13. *Interaction mode*	a. Issues and personal differences are skirted or repressed	a. Issues and personal differences are confronted and addressed openly
14. *Payoffs for good behavior*	a. Mainly monetary	a. Recognition, promotion, added responsibility, choice assignments, plus money
15. *Business ethics*	a. Ambivalent, rides the tide	a. Clearly defined and regularly followed
16. *Internal relationships*	a. Highly competitive, hostile	a. Friendly, competitive, supportive
17. *Values and beliefs*	a. Economic, political, self-centered	a. Social, spiritual, group-centered
18. *Success formula*	a. Works harder	a. Works smarter
19. *Human resources*	a. Burnout b. High turnover c. Grievances	a. Not enough promotional opportunities for all the talent b. Low turnover c. Job satisfaction
20. *Company loyalty*	a. Low	a. High
21. *Major financial concern*	a. Cash flow shortage	a. Opportunities for new investment
22. *Growth pattern*	a. Sporadic	a. Consistent
23. *Relationship with competitors*	a. Hostile	a. Professional

TABLE 1.1 *(continued)*

Variable	High Fraud Potential	Low Fraud Potential
24. Innovativeness	a. Copy cat, reactive	a. Leader, proactive
25. CEO characteristics	a. Swinger, braggart, self-interested, driver, insensitive to people, feared, insecure, gambler, impulsive, tight-fisted, numbers- and things-oriented, profit-seeker, vain, bombastic, highly emotional, partial, pretend to be more than they are	a. Professional, decisive, fast-paced, respected by peers, secure risk-taker, thoughtful, generous with personal time and money, people- products- and market-oriented, builder-helper, self-confident, composed, calm, deliberate, even disposition, fair, know who they are, what they are and where they are going
26. Management structure, systems and controls	a. Bureaucratic	a. Collegial
	b. Regimented	b. Systematic
	c. Inflexible	c. Open to change
	d. Imposed controls	d. Self-controlled
	e. Many-tiered structure, vertical	e. Flat structure, horizontal
	f. Everything documented, a rule for everything	f. Documentation is adequate but not burdensome, some discretion is afforded
27. Internal communication	a. Formal, written, stiff, pompous, ambiguous	a. Informal, oral, clear, friendly, open, candid
28. Peer relationships	a. Hostile, aggressive, rivalrous	a. Cooperative, friendly, trusting

1.3 INTERNAL CONTROLS AND "FRAUDPROOFING"

Developing an understanding of the various factors that contribute to the risk of fraud is only the first step in a fraud prevention strategy. Following this, it is necessary to implement policies that will help to reduce the threat.

Some of the measures that can guard against the threat of fraud were explained previously in this chapter. Consider what is perhaps the main, and certainly the most common, prevention tool: a good system of internal controls.

1.3.1 Defining Internal Control Objectives

In recent years, *fraudproofing* has appeared in the literature and some seminars. This term is somewhat misleading, however, because no internal control system can completely eliminate the risk of fraud. What fraud proofing should do, in theory, is reduce the risk of fraud to an acceptable level. If you have suffered from a fraud attack, consider interviewing the fraudster after the case is closed. Many fraudsters have a bit of braggadocio in them and, as a result, are only too willing to let you in on the very holes in your control system that they exploited.

The risk of fraud is not the only factor in defining internal control objectives; for example, management information and reporting requirements are important considerations as well. However, the acceptable levels of risk and opportunity, as defined in section 1.1.6 should also be considered. This means effectively combining the three levels of internal control—basic, supervisory, and audit (see sections 1.3.2–1.3.4)—to limit the risk of fraud to acceptable levels.

1.3.2 Basic Controls

A variety of basic controls exist in a typical system of internal controls. The most relevant basic controls are grouped into three categories: physical access, job descriptions, and accounting reconciliations and analyses.

Physical Access

Most people acknowledge the need to control physical access to valuable assets including intangible assets such as information. Measures to control physical access include the obvious practice of locking doors, desks, and file cabinets so that unauthorized personnel, either within or outside the organization, cannot gain access. Other measures include employee IDs and passwords, computerized security systems (for example, access cards that record time of entry and exit), and electronic surveillance systems, which should include every new innovation, such as biometrics–including, for example, iris scans and voice recognition–that the business can afford.

As a general rule, organizations should restrict physical access to those who require it to perform their job function. Of course, controlling physical access in this way will not completely reduce the risk of fraud. However, it will help to reduce the risk in the following ways:

- Many frauds require that the perpetrator come into physical contact with either the asset being misappropriated, or the related asset records, in order to conceal the fraud. Reducing physical access reduces opportunity.
- Physical access controls are often the most visible to potential perpetrators. Strong controls in this area send a powerful deterrent message vis-à-vis the other controls in the system. Conversely, loose physical controls invite challenge.
- Access controls that do not prevent fraud often assist in the fraud investigation process (for example, determining what actually happened and narrowing down suspects).

Carefully screening who had access to cash receipts would have saved one U.S. County Clerk much grief. According to a newspaper report, a temporary employee was stationed at the front desk to handle passport applications, including collecting the necessary fees. The temp properly recorded and submitted for processing those applications paid for by check or money order. She pocketed any cash received and destroyed all evidence of the cash applications so that there was no record of the transaction. Not paying attention to controlling physical access led to several thousands of dollars in losses.

Job Descriptions

Formal, specific job descriptions are a very effective fraud prevention tool. These descriptions should spell out exactly what is expected of each employee. Generally, employees should not perform duties outside their job description. Those who do, represent a significant red flag.

Create job descriptions that reflect the important principle of division of duties. For example, employees with physical control over an asset should not also keep the records relating to that asset (this will only make it easier for them to cover up the fraud). Segregate all other especially sensitive duties—for example purchasing and check signing.

The need for job descriptions goes beyond the widely recognized concept of segregating duties, although it is certainly one of the important consequences of job descriptions. Some cases may result in an entirely appropriate duplication of duties, for example, double signing checks. Specify in the job description that all employees *must* take annual vacations (another well known fraud prevention tool, because an employer can more likely discover perpetrators running an ongoing fraud scheme when they're removed from the scene).

Thus, it is apparent that employers must approach the process of formulating job descriptions for their employees in an integrated fashion. From an internal-control and fraud-prevention perspective, different tasks performed by different individuals may be interrelated; therefore, an appropriate job description for one employee will often depend on the job descriptions of others, and vice versa.

Employers often ignore or underestimate the need for formal job descriptions, writing them off as "more useless paper." At other times, employers create job descriptions but then ignore them. This attitude invites trouble. As one leading fraud investigator put it: "When people begin to do things outside their job description, you have reason to be concerned. If it goes unrewarded, they begin to develop a justification to steal. It's very important that job descriptions are clear, agreed upon, and adhered to."

Accounting Reconciliations and Analyses

After access controls and job descriptions, accounting reconciliations and analyses are the third most important group of basic controls. An essential ingredient of a successful fraud is successful concealment. Regular, appropriately performed accounting reconciliations and analyses often make such concealment difficult or impossible.

Perform accounting reconciliations regularly (for example, monthly basis) including:

- Bank reconciliations, for all accounts
- Accounts receivable reconciliations (both month to month and general ledger to subledger)
- Accounts payable reconciliations (again, both month to month and general ledger to subledger)

The exact nature of the accounting analyses performed depends on the nature of the organization's operations. Analyses relevant for most organizations include:

- Variance analysis of general ledger accounts (budget to actual, current year versus prior year, and so on)
- Vertical analysis of profit and loss accounts (that is, calculation of expenses as a percentage of sales, and comparison of these percentages with historical standards, or budgets, or both)
- Detailed sales and major expense analyses (for example, by product line or territory)

Of course, organizations often undertake accounting reconciliations and analyses with other purposes in mind—for example, to make management decisions or to ensure the accuracy of the accounting records, or both. Nevertheless, this process also can highlight discrepancies that point to fraud.

1.3.3 Supervision

Supervision represents the second level of internal control. From a fraud prevention perspective, strong supervision is vital—especially in small businesses that may have difficulty achieving segregation of duties.

Note that active supervision most definitely differs from supervisory or management override, in which a manager or supervisor actually takes charge of or alters the work of a subordinate. In fact, override itself is a red flag—that is, it suggests that the manager or supervisor may be engaged in fraud or the concealment of one. Allow basic controls to operate as they were intended, rather than to be circumvented by those at higher levels.

As a fraud prevention mechanism, good supervision consists of:

- Fraud awareness
- Approval, review, double-checking and redoing

Fraud Awareness

Fraud prevention specialists constantly emphasize the need for "fraud awareness," to the point that the term has almost become a cliché. However, such awareness is perhaps the key prerequisite in building any effective fraud prevention strategy, and is especially important at the supervisory level.

Specifically, supervisors must be alert to the *possibility* of fraud whenever an unusual or exceptional situation occurs, such as complaints from suppliers or customers, discrepancies that don't make sense, or accounting reconciliations that don't balance. If a manager's mind is closed to the possibility of fraud during an unusual or exceptional situation, the risk of the fraud continuing unabated greatly increases.

Several businesses have had positive results in raising employees' awareness by publishing regular internal newsletters. In addition to reporting actual fraudulent activities, the newsletters relate the impact of the fraud on both the employees and the bottom line.

Approval, Review, Double-checking and Redoing

In addition to awareness, fraud prevention demands that supervisors actually supervise. This means going beyond the typical approval function, such as initialing invoices or performing other duties of supervisors and managers. A more thorough review, double-checking employees' work, and redoing some tasks, may be necessary and should be approached diligently. For example, assign supervisors the responsibility of double-checking important procedures such as the monthly bank reconciliation—that is, comparing the numbers on the bank reconciliations to those on the bank statements and in the general ledger, making certain those numbers total correctly, test-checking outstanding items at the very least, and so on. To simply initial bank reconciliations in a habitual or reflex-like manner without really reviewing and actually redoing them invites fraud.

For example, the owner of a busy downtown restaurant used the following system of internal control for sales. Employees entered all prenumbered customer bills into the cash register, and at least once each day the hostess/bookkeeper batched the customer bills, listed them on a deposit sheet, and made the related bank deposit. The owner then matched the totals on the deposit sheet with the amounts shown in the stamped deposit book, and believed this to be adequate supervision.

The owner's supervision of the bookkeeper, however, was inadequate especially because she was responsible for handling the cash (the bank deposit) and related records (customer bills, cash register tapes, deposit sheets). In fact, over a three-month period, the bookkeeper

(Text continued on page 21)

skimmed a portion of each day's cash receipts by omitting some of the cash sales bills and pocketing the corresponding amounts. The owner might have uncovered the fraud by using any one of the following methods:

- *Segregating duties*: The owner rejected this method because he trusted the bookkeeper and did not want to incur the cost of an additional employee.
- *Accounting for all prenumbered bills*: The owner opted not to use prenumbered bills because it was too time-consuming. The bookkeeper intentionally did not list the bills in numbered order on the deposit sheet and prenumbered books were issued out of sequence to waiters and waitresses.
- *Matching daily cash register tapes to the daily cash deposit*: The owner rejected this simplest and most appropriate method; not wanting to check his employee's work in this way because the tapes were a messy "dog's breakfast" kept in a shoe box by the bookkeeper, entirely by design, of course, to cover up the fraud.

The owner eventually uncovered the fraud when the bookkeeper became too greedy and withheld a bit too much from what the owner knew was an especially good cash sales day, which raised his suspicions and lead to an investigation.

This example illustrates the necessity of supervision: often it is the primary defense against ongoing frauds such as the skimming of cash or the lapping of accounts receivable. The maximum opportunity level for the bookkeeper in the previous example should have been the outright theft of the day's cash receipts—typically less than half of a day's total receipts of about $10,000. However, inadequate supervision allowed a smaller amount of cash—about $700 a day—to be stolen over a period of three months, which amounted to a total loss of over $60,000.

1.3.4 Audit

From a fraud-prevention perspective, audit represents the third level of an organization's internal control system.

Internal Audit

Internal auditors work for the organization and perform the kinds of work defined by senior management. In this sense, internal auditors are an extension of senior management—they have the same concerns and deal with the same issues described throughout this chapter. Therefore, their work might include fraud detection, or developing fraud prevention mechanisms, or both.

The training programs and available literature for internal auditors—as provided by the Institute of Internal Auditors (IIA)—pay specific attention to the issue of fraud prevention and detection. Historically the perspective of internal auditors differs from that of the external auditors, which is described below.

External Audit

External auditors are independent of the organization. They report on financial statements and perform other independent reviews. The restricted role of the external auditor has evolved over time. During the late 1800s and into the early 1900s, auditors actively looked for fraud—to be a kind of "bloodhound." Court rulings redefined their role to that of a "watchdog." Today, auditors are expected to bark if they see something suspicious, but they are not expected to sniff around for things that might be suspicious.

This watchdog metaphor has persisted throughout most of the twentieth century. In particular, the concept of materiality has played an important part in the accounting profession's view of fraud, which is, specifically, that an auditor's procedures cannot be expected to detect immaterial frauds. No audit can be expected to give absolute assurances in this area, and even limited assurances would require procedures so extensive that the audit would be uneconomical. If a fraud is material enough to affect the financial statements of an organization—and an auditor's opinion on those financial statements—then the auditor's procedures may uncover it. However, there is certainly no guarantee of detection. For example, even when the auditor's procedures are sound, the perpetrator(s) may go to extensive lengths to deceive the auditor and hide the defalcation.

In recent years, the public's expectations has reopened to some extent the bloodhound-watchdog debate primarily because of the perception that auditors should bear responsibility for detecting significant frauds even when immaterial to the total worth of an organization.

1.4 Detecting and Preventing Fraud in Books of Account

1.4.1 The Auditor's Duty to Detect Fraud

Shortly after human beings became rational animals, their thinking skills were enhanced by the ability to rationalize. Unfortunately, this led to lying and cheating. Today, lying and cheating are commonly labeled fraud. Accordingly, humans have a long history of both committing frauds and being victims of fraud.

Accountants and auditors have had to contend with dishonest practices in accounting records since commerce was first recorded and bookkeeping became a double-entry process of recording. Since that time, we have needed accountants to make such double entries and auditors to assure the accuracy of their entries.

In addition to the auditor's duty to determine whether entries are made accurately, historically auditors have had a corollary responsibility to determine whether any entries were false (that is, fraudulent). But not everyone agreed that the latter was the peculiar province of the auditor. Some found management primarily responsible for detecting fraud in the accounting records. At its discretion, management could delegate that duty to auditors.

Most outside auditors do not accept responsibility for detecting fraud in the usual course of independent audits. But despite their protestations, many courts have suggested that independent auditors be given such a duty. These precedents were established in cases in which outside auditors were the targets of regulatory agencies. In these suits, courts have ruled that outside auditors have a duty to detect fraud in the accounting records, but only to the point where clients actively have attempted to deceive the outside auditors by concealing fraudulent transactions or entries. Federal courts seem to hold auditors to a higher duty of professional care than do State courts. But even State courts tend to impose a duty to detect fraud under some circumstances. In fact, a large number of professional malpractice suits brought against outside auditors in State courts involve allegations of undetected embezzlement.

Other distinguishing characteristics of the businesses most frequently involved in malpractice suits include:

- Nonpublic, small, family owned enterprises
- One-person, unbonded bookkeeping staff with loose internal controls
- Poor prospects of business survival and a chronic cash flow shortage
- Inactive or incompetent management and a high rate of turnover of outside audit firms
- Engaging an auditor to review or compile rather than to audit.

1.4.2 Fraud and Statement on Auditing Standards (SAS) No. 82

Consideration of Fraud in a Financial Statement Audit

Fraud detection is not the primary objective of a financial statement audit. Yet the auditors' responsibility for detecting fraud is increasingly controversial. This is due, in part, to the *expectation gap.*

The expectation gap is the difference between what the public expects auditors *do* and what auditors *in fact, do.* In other words, the public remains ignorant of the extent of the auditors' responsibilities. This contrasts with the limitations of what auditors can reasonably expect to achieve. The average person's exposure to what an accountant or auditor does is usually limited to the tax season or tax audits. Accordingly, the general public, regardless of the efforts by the AICPA and other professional groups, still lacks a true perception of the role of the auditor.

Auditors should be fully aware of their responsibilities under the AICPA's Statement on Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit.* This SAS was issued in February of 1997 and superceded SAS 53, entitled *The Auditors Responsibility to Detect and Report Errors and Irregularities.*

According to SAS No. 53, "Since the auditors opinion on the financial statements is based on the concept of reasonable assurance, the auditor is not an insurer and his report does not constitute a guarantee." While auditors agree with this statement, the public, due in large part to the expectation gap, may not agree.

As stated in SAS No. 82, the auditor should consider the risk that the financial statements are materially misstated due either to unintentional error or fraud. Accordingly, the auditor must specifically consider factors that bear on the likelihood of fraud. The level of risk assessed may affect engagement staffing, extent of supervision, overall strategy, and the degree of professional skepticism applied.

Auditors' Responsibility

SAS No. 82, in amending SAS No. 53, states, in part: "When considering the auditor's responsibility to obtain reasonable assurance that the financial statements are free from material misstatement, there is no important distinction between errors and fraud." In other words, the auditor is responsible for planning the audit to detect material misstatements due to fraud. SAS No. 82 does not increase the auditor's responsibility for the detection of material misstatement due to fraud, but rather makes clear the responsibility that previously existed. According to SAS No. 82, an auditor should do the following:

- Assess the risk of material misstatement of the financial statements due to fraud and consider that assessment in designing audit procedures.
- Inquire of management about its understanding of the risk of fraud and its knowledge of frauds perpetrated on or within the organization.
- Plan and perform the audit to achieve reasonable assurance of detecting material misstatement of the financial statements due to fraud.
- Consider whether misstatements detected during the audit are the result of fraud and, if so, evaluate the implications and communicate the matter to appropriate client personnel.
- Document the facts that evidence the auditor's assessment of the risk of fraud and the auditor's response to the risks identified.

Types of Fraud

The misstatements most relevant to an audit of financial statements originate from two types of fraud:

1. *Fraudulent financial reporting*: The client intentionally misstates the financial statements through phony accounting records or documents, misrepresentation or omission of significant information, or misapplication of accounting principles. Fraudulent management usually directs or performs these activities.
2. *Misappropriation of assets*: Client personnel steal entity assets and conceal the theft through misstatement of financial records. Fraudulent employees usually perform these activities.

The auditor has no responsibility for detection of misstatements, whether caused by error or fraud, that are not material to the financial statements. For example, misappropriation of assets often is not material to the financial statements. However, the client might incorrectly expect that the auditor should detect all cases of fraud, whether or not the financial statements are materially misstated.

1.4.3 Fraud Auditing versus Financial Statement Auditing

Financial statement auditing is a methodology for evaluating the level of accuracy, timeliness and completeness of the recordings of business transactions. However, auditors do not review all transactions. Auditors use sampling and confirmation techniques to test accuracy, timeliness and completeness. The purpose of testing is to determine whether transaction data are free of material error and to confirm that financial statements accordingly are free of material misstatement.

Fraud auditing, while borrowing many techniques from financial statement auditing, is more a mindset than a methodology. It relies on creativity (right-brain thinking) as much as it does on reasoning (left-brain thinking). It requires that the fraud auditor think, but not act, like a thief by considering the following:

- Where are the weakest links in the chain of controls?
- How can the controls be attacked without drawing attention?
- How can thieves destroy the evidence of their attack?

- What powers can the thieves enlarge?
- What plausible explanation can thieves give if someone suspects their activities?
- How can fraudsters, if apprehended, explain their conduct?

The more fraud auditors can learn to think like thieves, the more effective their efforts will be in detecting fraud.

Financial statement and fraud auditing also differ in the degree of concern for evidence of material error or misstatement. While the materiality rule in financial statement auditing has its place in a cost-benefit context, materiality is not a guiding principle in fraud auditing. The amount of a visible fraud may be small, but frauds in books of account can be like icebergs—the biggest part is below the surface. Discovering even small discrepancies can reveal large defalcations. That's one reason why auditors often say they discover fraud by accident, not by audit plan or design. In truth, the "discovery" of fraud is generally no accident. It comes from diligent effort and a basic assumption by auditors that if fraud exists, they will find it.

Are all frauds in the accounting records discovered on the basis of undetected discrepancies? No. Many frauds surface on the basis of allegations or complaints by coworkers, coconspirators, customers, competitors, suppliers, or prospective suppliers.

1.4.4 Fraud Auditors versus Financial Statement Auditors

Skills of fraud auditors include:

- Reconstructing financial transactions through third-party sources
- Gathering and preserving accounting evidence for trial
- Testifying as expert witnesses
- Calculating net worth and living expenses
- Inspecting documents for authenticity, alteration, forgery and counterfeiting
- Documenting a fraud case for criminal, civil, and insurance claim purposes
- Designing fraud scenarios, that is, imagining what a criminal might think and do in situations where internal controls are loose or not enforced and the criminal has certain powers and authority over assets and accounting records

What distinguishes fraud auditors from financial statement auditors? In most respects, they are the same. Financial statement auditors are in their element when books and records are complete and reasonably accurate. Fraud auditors must make order out of what looks like chaos in books and records. Most of the supporting documents the fraud auditor must access for confirmation lie in the hands of third parties who might be reluctant to assist in the audit effort.

Fraud auditors tend to be right-brain thinkers, that is, more creative than rational in their thought processes. In that context, they may understand the inner workings of the criminal mind somewhat better because many criminals are not noted for orderly, rational or systematic thinking. Criminals are often of the "hit and run" variety—neither planning their crimes thoroughly nor anticipating the consequences of getting caught. They want the "big score" now. Most embezzlers, however, tend to be left brain thinkers, that is, known for their reasoning abilities, who will steal small sums over an extended period of time.

1.4.5 The Risk of Fraud

Some organizations suffer more fraud than others. What increases the risk or exposure to loss from fraud in any organization? The answer depends on a number of factors. The incidence of fraud in the accounting records is distributed unevenly. Some industries, some companies, some occupations, and some individuals are higher risks than others.

High-risk industries are noted for intense rivalry, low profits, and unethical business practices. Some members of these industries are controlled by underworld figures and may enjoy sweetheart arrangements with corrupt labor unions. Disputes are often settled by bribes, or, when necessary, by force.

High-risk companies are noted for poor management, loose controls, loose cash, and loose business morality.

High-risk occupations provide easy access to cash and accounting records, and are often characterized by low pay, long hours and job-related stress.

High-risk individuals are financially overburdened people with low self-esteems, addictive personalities (gambling, substance abuse, high living), are poor managers of their financial resources, have worked their way into positions of trust, and rationalize their thefts as "borrowing" or getting even for imagined exploitation. Such people often work long hours at their own discretion, and take no vacations for fear their defalcations might be discovered while they are away. A growing number of these thieves also keep elaborate records of their thefts. The records usually contain dates, amounts, and details of the conditions in their lives at the time the cash or property was taken. It is believed that such scrupulous bookkeeping is a defensive ploy. If they get caught, they think they can make a credible defense of their intention to return the money or property. This defense may cast doubt on one element of proof needed to convict: the intent to permanently deprive the owners of their property.

People commit crimes for a number of reasons. The main motives are economic, egocentric, ideological, and psychotic. The economic motive (need or greed) is the most common one found for the crimes of fraud, theft, and embezzlement.

In large corporations, with promotional policies and compensation plans geared to short-term bottom-line results and little else, a form of competitive greed can set in at the profit-center management level. Even well managed companies have become victims of their own compensation designs. Therefore, falsifications of unit profits, revenues and expenses have become a greater problem in the U.S. corporate landscape.

1.5 Risk Management Checklist

Table 1.2, Risk Management Checklist, is designed to assist CPAs in assessing and managing the risk of fraud in their organizations and in those of their clients. Generally, all **NO** answers require investigation and follow-up, the results of which should be documented. Use the *Ref* column to cross-reference any additional documentation to the appropriate work papers.

The checklist is intended for general guidance and information only. Use of the checklist does not guarantee the prevention or detection of fraud and is not intended as a substitute for audit or similar procedures. Those with vital concerns about fraud prevention or who suspect fraud should seek the advice of a competent fraud practitioner.

TABLE 1.2 RISK MANAGEMENT CHECKLIST

Risk Management Checklist	Yes	No	NA	Ref
1. Does the organization have an adequate level of fraud awareness and are appropriate policies in place to minimize fraud risk, specifically:				
a. Generic risk factors				
• Has the organization assigned each employee a maximum "opportunity level" to commit fraud, that is, has management asked itself the question, "What is the maximum amount this employee could defraud the organization, and does this represent an acceptable risk?"	☐	☐	☐	___
• Has the organization set a catastrophic opportunity level; that is, has management asked itself the question, "Have we ensured that no single employee—or group of employees in collusion—can commit a fraud that would place the organization in imminent risk of survival?"	☐	☐	☐	___
• Does the organization have a policy of immediately dismissing any employee who has committed fraud?	☐	☐	☐	___
• Does the organization have a policy of reporting all frauds to the authorities and pressing charges?	☐	☐	☐	___
• For all frauds experienced by the organization in the past, has management evaluated the reasons that led to the fraud and taken corrective action?	☐	☐	☐	___
b. Individual risk factors				
• Does the organization have a corporate mission statement, which includes as an objective good citizenship, that is, the maintenance of good standing in the community?	☐	☐	☐	___
• Does the organization have a written code of ethics and business conduct (see checklist in chapter 2 for details)?	☐	☐	☐	___
• Does the organization conduct ethical and security training for new employees and periodic updates for existing employees?	☐	☐	☐	___

(continued)

TABLE 1.2 *(continued)*

Risk Management Checklist	Yes	No	NA	Ref
• Does management set the right example; that is, does it follow the organization's mission statement, code of ethics and business conduct, and other policies of the organization, and is it clearly seen to be doing so by employees?	☐	☐	☐	___
• Does the organization's culture avoid characteristics that promote unethical behavior, for example, high or even hostile competitiveness within the organization that might push employees to the point of burnout; pointless rigid or petty policies, or both; over-centralization of authority?	☐	☐	☐	___
• Do the organization's hiring policies, to the extent possible, seek out individuals of high moral character and weed out those of low moral character (see checklist in chapter 3)?	☐	☐	☐	___
• Does the organization use for especially sensitive positions screening or testing procedures, or both; for example, psychological tests, drug tests, or lie detector tests, or a combination of all three, where permitted by law?	☐	☐	☐	___
• Does the organization provide or encourage counseling, or both, for employees with personal problems, for example, alcohol and drug abuse?	☐	☐	☐	___
• Does the organization have fair policies in the area of employee relations and compensation, for example, salaries, fringe benefits, performance appraisal, promotions, severance pay, and do these policies compare favorably with those of competitors and promote an environment that minimizes disenchantment and other similar motives to commit fraud?	☐	☐	☐	___
• Does the organization have fair mechanisms in place for dealing with employee grievances?	☐	☐	☐	___
• Does the organization, as a feedback mechanism concerning employee relations' policies, conduct exit interviews with departing employees?	☐	☐	☐	___
c. Overall risk factors				
• Does the organization exhibit an awareness of fraud and its possible manifestations, for example, signs of employee problems such as drug addictions, the low paid employee who suddenly appears with the trappings of wealth, and so on?	☐	☐	☐	___

TABLE 1.2 *(continued)*

Risk Management Checklist	Yes	No	NA	Ref
2. Does the organization have an adequate system of internal controls, specifically:				
a. Internal control				
• Has the organization explicitly considered the need for fraud prevention in the design and maintenance of the system of internal controls?	☐	☐	☐	___
b. Control over physical- and logical-access				
• Does the organization have a policy of locking doors, desks, and cabinets after hours and when unattended, especially in areas with valuable assets including files and records, for example, personnel and payroll, customer and vendor lists, corporate strategies, marketing plans, research?	☐	☐	☐	___
• Does the organization use IDs and passwords, for example, for computer files?	☐	☐	☐	___
• Does the organization state and enforce a policy that restricts access to those requiring it for job performance, including a strict policy against employees allowing access to unauthorized personnel, for example, by loaning keys or sharing passwords?	☐	☐	☐	___
• Has the organization installed, for especially sensitive areas, computerized security or electronic surveillance systems, or both?	☐	☐	☐	___
• Does the workplace *appear* to an impartial observer to have adequate access controls?	☐	☐	☐	___
c. Job descriptions				
• Does the organization have written, specific job descriptions?	☐	☐	☐	___
• Are job descriptions adhered to?	☐	☐	☐	___
• Does the organization have an organization chart that reflects and is consistent with the job descriptions of its employees?	☐	☐	☐	___
• Are incompatible duties segregated, for example, handling of valuable assets—especially cash—and related records?	☐	☐	☐	___

(continued)

TABLE 1.2 *(continued)*

Risk Management Checklist	Yes	No	NA	Ref
• Does the organization properly segregate the purchasing functions, that is, ensuring that one individual cannot requisition goods or services, approve and make the related payment, and access accounts payable records?	☐	☐	☐	___
• Are especially sensitive duties duplicated, for example, the double-signing of checks over a specified amount?	☐	☐	☐	___
• Do job descriptions specify that employees must take annual vacations?	☐	☐	☐	___
• Is the overall process of formulating job descriptions integrated with adequate consideration to the importance of fraud prevention?	☐	☐	☐	___
d. Regular accounting reconciliations and analyses				
• Are all bank accounts reconciled?	☐	☐	☐	___
• Are all accounts receivable reconciled, for example, month to month, general ledger to subledger?	☐	☐	☐	___
• Are all accounts payable reconciled, for example, month to month, general ledger to subledger?	☐	☐	☐	___
• Has the organization performed a variance analysis of general ledger accounts, for example, budget to actual, current year versus prior year?	☐	☐	☐	___
• Has the organization performed a vertical analysis of profit and loss accounts, that is, as a percentage of sales against historical or budget standards, or both?	☐	☐	☐	___
• Has the organization performed an analysis of detailed sales and major expenses, for example, by product line or geographic territory?	☐	☐	☐	___
e. Supervision				
• Do supervisors and managers have adequate fraud awareness, that is, are they alert to the *possibility* of fraud whenever an unusual or exceptional situation occurs, such as supplier or customer complaints about their accounts?	☐	☐	☐	___
• Do supervisors and managers diligently review their subordinates' work, for example, accounting reconciliations, and redo the work when appropriate?	☐	☐	☐	___

TABLE 1.2 *(continued)*

Risk Management Checklist	Yes	No	NA	Ref
• Does close supervision adequately compensate against the increased risk of fraud in smaller businesses or where an inability to divide duties exists.	☐	☐	☐	___
• Is supervisory or management override, that is, a manager or supervisor taking charge of, altering, or otherwise interfering in the work of a subordinate prohibited, and are others in the hierarchy alert to this situation as a fraud red flag?	☐	☐	☐	___
f. Audit				
• Is there an internal audit function?	☐	☐	☐	___
• Does the internal audit function perform regular checks to ensure that fraud prevention mechanisms are in place and operating as intended?	☐	☐	☐	___
• Are external audits performed on a regular basis, for example, quarterly for larger businesses?	☐	☐	☐	___
• Do external auditors receive full cooperation from management with respect to their work in general and fraud matters in particular, for example, through the audit committee?	☐	☐	☐	___
3. Has the organization specifically addressed the following fraud prevention issues:				
a. Ethical Environment	☐	☐	☐	___
b. Risk Financing	☐	☐	☐	___
c. Computer Security	☐	☐	☐	___

Promoting an Ethical Environment

CHAPTER 2:

Promoting an Ethical Environment

CHAPTER 2:

Promoting an Ethical Environment

2.1 ETHICS: A FRAMEWORK

An ethical environment is a key element in any effective prevention strategy. This chapter will acquaint you with the field of applied ethics, provide essential tools for promoting an ethical environment within an organization, and conclude with a diagnostic tool that you can use when evaluating an organization's current ethical status.

2.1.1 Overview

Ethics—derived from the Greek *ethos,* meaning character or custom—is a very broad term referring to principles or standards of human conduct. Ethics has been, and continues to be, one of the key concerns of all religions, schools of philosophy, sciences, liberal arts, professions, and political movements. Moses, Confucius, Plato, Aristotle, Kanto, and many others devoted a great deal of their recorded teachings to the subject of ethics. It is impossible to engage in any human endeavor, including business, without entering the field of ethics.

Applied Ethics

Applied ethics is the science devoted to the study of the "walk," rather than the talk, of ethics. According to Lisa H. Newton, in her text *Doing Good and Avoiding Evil: Principles and Reasoning of Applied Ethics,* "Applied ethics, then, is the field that holds ethical theory accountable to practice and professional and business practice accountable to theory." It's where the rubber meets the road.

Personal Versus Organizational Ethics

Whose principles and standards should we adopt? There remains much confusion about this fundamental question. Some believe that ethics are a matter of personal choice. Therefore, any attempt to establish a code of ethics, or conduct, would result in a narrow flight of parochial fancy that would be so patently offensive to so many, it would render itself immediately irrelevant. Others believe that a kind of universal genetic code of ethics or conduct exists. This theory suggests that we are all born with an inherent sense of right and wrong. So, any artificial code of ethics is unnecessary and would be flawed in any way in which it conflicted with the natural code. Both groups believe it would be wrong for any organization to impose ethical standards on its members, employees, or other stakeholders. Nothing could be further from the truth.

It is an organization's right and duty to clearly communicate its values and expectations regarding the conduct of its affairs to all its stakeholders. Employees or members may freely choose to join, or not to join, any given organization. But, once individuals choose to join an organization, they assume a duty to respect the organization's values and abide by its code of conduct.

Ethics and the Law

When confronted about unethical behavior, many people will point out that their actions were not illegal. This would be roughly analogous to saying that because a person follows the rules of law, he or she would be an excellent judge. According to the *Professional Ethics for Certified Public Accountants* (a publication of the California Certified Public Accountants Foundation for Education and Research) "Laws and rules establish minimum standards of consensus impropriety; they do not define the criteria of ethical behavior."

2.1.2 Ethics at Work

In the Professions

Most, if not all, recognized professions have developed written codes of ethics, professional conduct, or both. They also have implemented means to assure that members of the profession abide by these codes. Violators are usually disciplined or expelled, sometimes in public proceedings, to demonstrate the profession's commitment to its code and willingness to effectively police itself.

Some would argue that the professions became interested in ethics for entirely selfish reasons. They see the rise of successful plaintiffs' litigation in the 1970s as a key motivator in the promulgation of professional codes of ethics and conduct. They also point out that, during the 1980s and 1990s, the federal government demonstrated an interest in playing an increased role, including the actual promulgation of codes of conduct, in the regulation of professions. The AICPA has written and rewritten its code of professional conduct many times during the past 100 years or so. In fact, according to *Professional Ethics for Certified Public Accountants,* a complete restatement of the code was made in 1973.

Whatever the motivation, professional codes of conduct have been effective. The reason is simple: if you do not abide by the ethics code of your profession, you lose the right to practice and earn a living. Coupling this reason with the profession's corporate interest in maintaining its standing and authority, thus minimizing its exposure to litigation and intrusion by the government, demonstrates the steps taken toward promoting an ethical environment.

But, how do we apply this model to businesses, including professional firms?

Business Ethics

Should business be concerned with ethics? The answer was not always a unanimous *yes.* Who hasn't heard the appropriated maxim: All is fair in love and business. You may recall Shakespeare's merchant and Dickens' Fagan as examples of at least the perception of business motives in western society. In this country, tales of the robber barons of the nineteenth century suggest that business ethics were not at the top of the enterprise success-factor list. That was then, but what about now? As recently as the 1970s, mainstream economist Milton Friedman said that the only obligation of a business is to make a profit. This became dogma in American business schools in the 1970s and 1980s.

So, why should business be concerned with ethics today? One could argue that after November 1991—the effective date of the federal sentencing guidelines for organizations—business became concerned with ethics in order to guard against huge fines and penalties. But there are other, pragmatic reasons for business to be concerned with ethics:

Enlightened self-interest. According to the *Professional Ethics for Certified Public Accountants*, a business needs to avoid scandals, keep government off its back, protect itself from internal corruption, avoid fines and penalties, and keep its executives out of jail. Also, there is the value of a good corporate image, the internal cost of investigations and legal fees, the value of good employee morale, and the impact of wrongdoing on the share value of public companies to consider. In fact, ethics may have a great deal more to do with making a profit than Mr. Friedman imagined.

2.1.3 Promoting an Ethical Environment

The Tone at the Top

You've heard it before and it must be said again. The tone of upper management is most important in the field of ethics. Ethics will not suffer senior management's clever rationalization or thinly veiled hypocrisy. Fortunately, or unfortunately, ethics always comes down to a simple choice of right over wrong. Even the most learned defense of improper conduct in the executive suite would fail the ethics test. If the bosses aren't ready to walk the talk, the process simply will not work.

Senior management must be made aware of this essential element. Some will raise objections about the cost of an ethics program or its potential negative impact on revenue. Even today, the best way to communicate the value of an effective ethics program is to quantify the cost of not having an ethics program. Statistics and examples abound. According to an Association of Certified Fraud Examiners report, it was estimated that in 1996 U.S. organizations lost over $400 billion to occupational fraud and abuse. But, to bring the point home, you need look no further than your favorite daily business journal. Virtually every issue contains stories of businesses and other organizations that have been victimized through fraud and paid dearly for it. Those businesses that allegedly "benefited" from the fraud end up losing the most.

The Current Situation

All ethics, like all politics, are local. Resist the temptation to run out and "buy" someone else's ethics program for your organization. An ethical environment flows from an ethics program that is tailored to the organization. If you try to develop a rule in advance for every situation, you will fail. If you try to fix things that are not broken, you will fail. Finally, if in the process of installing your new, super-deluxe, off-the-shelf ethics program, you communicate your distrust of employees and other stakeholders to them, they, in turn, will justify that distrust.

For all of these reasons, begin by analyzing your individual organization. Involve everyone in the process. Get their input. Develop a brief statement (mission statement) of the organization's core values and mission.

Perform a diagnostic to identify weak and strong areas of ethical conduct within the organization. You should consider using the Ethical Environmental Checklist at the end of this chapter, or you could use this checklist as a template to develop a diagnostic tool of your own. Once you compile the results of your diagnostic exercise, analyze the results, make any necessary decisions, and begin designing the program.

Designing the Ethics Program

The most important requirement when promoting an ethical environment is having a written code of ethics and business conduct. A written code helps to set the right ethical tone within an organization. Figure 2-1 is an example of a written mission statement.

Figure 2-1. A Written Mission Statement

Mission Statement

The Organization's mission is to provide the highest quality goods and services to its customers; to strive at all times for market leadership and in so doing, to benefit the Organization's shareholders and its employees.

The Organization is committed to a policy of fair dealing and integrity in the conduct of all aspects of its business. This commitment is based on a fundamental belief in law, honesty and fairness. The Organization expects its employees to share its commitment to high legal, ethical and moral standards.

This Code of Business Conduct is mandatory, and the Organization expects full compliance by all of its employees and by its subsidiaries under all circumstances. The Organization will monitor compliance, and any violation of the Code may result in disciplinary action that could include termination of employment.

Employees uncertain about the application of the Code should consult with their superior. Similarly any employee who becomes aware of, or suspects, a contravention of the Code, must promptly advise his or her superior, or report the matter directly to Human Resources, Internal Audit or the Law Department.

Figure 2-2 is an example of an organizational code of conduct, which includes definitions of what is considered unacceptable, and the consequences of any breaches thereof. Note that figure 2-2 is only an example. The specific content and areas addressed in your mission statement and code should flow from your own analysis of your organization.

Figure 2-2. An Organizational Code of Conduct

Organizational Code of Conduct

The Organization and its employees must, at all times, comply with all applicable laws and regulations. The Organization will not condone the activities of employees who achieve results through violation of the law or unethical business dealings. This includes any payments for illegal acts, indirect contributions, rebates and bribery. The Organization does not permit any activity that fails to stand the closest possible public scrutiny.

All business conduct should be well above the minimum standards required by law. Accordingly, employees must ensure that their actions cannot be interpreted as being, in any way, in contravention of the laws and regulations governing the Organization's worldwide operations.

Employees uncertain about the application or interpretation of any legal requirements should refer the matter to their superior, who, if necessary, should seek the advice of the Law Department.

General Employee Conduct

The Organization expects its employees to conduct themselves in a businesslike manner. Drinking, gambling, fighting, swearing and similar unprofessional activities are strictly prohibited while on the job.

Employees must not engage in sexual harassment, or conduct themselves in a way that could be construed as such, for example, by using inappropriate language, keeping or posting inappropriate materials in their work area, or accessing inappropriate materials on their computer.

Conflicts of Interest

The Organization expects that employees will perform their duties conscientiously, honestly and in accordance with the best interests of the Organization. Employees must not use their position or the knowledge gained as a result of their position for private or personal advantage. Regardless of the circumstances, if employees sense that a course of action they have pursued, are presently pursuing or are contemplating pursuing may involve them in a conflict of interest with their employer, they should immediately communicate all the facts to their superior.

Outside Activities, Employment and Directorships

All employees share a serious responsibility for an Organization's good public relations, especially at the community level. Their readiness to help with religious, charitable, educational and civic activities brings credit to the Organization and is encouraged. Employees must, however, avoid acquiring any business interest or participating in any other activity outside the Organization that would, or would appear to—

(continued)

Figure 2-2. *(continued)*

- Create an excessive demand upon their time and attention, thus depriving the Organization of their best efforts on the job.
- Create a conflict of interest—an obligation, interest or distraction—that may interfere with the independent exercise of judgment in the Organization's best interest.

Relationships with Clients and Suppliers

Employees should avoid investing in or acquiring a financial interest for their own accounts in any business organization that has a contractual relationship with the Organization, or that provides goods or services, or both to the Organization, if such investment or interest could influence or create the impression of influencing their decisions in the performance of their duties on behalf of the Organization.

Gifts, Entertainment and Favors

Employees must not accept entertainment, gifts, or personal favors that could, in any way, influence, or appear to influence, business decisions in favor of any person or organization with whom or with which the Organization has, or is likely to have, business dealings. Similarly, employees must not accept any other preferential treatment under these circumstances because their position with the Organization might be inclined to, or be perceived to, place them under obligation.

Kickbacks and Secret Commissions

Regarding the Organization's business activities, employees may not receive payment or compensation of any kind, except as authorized under the Organization's remuneration policies. In particular, the Organization strictly prohibits the acceptance of kickbacks and secret commissions from suppliers or others. Any breach of this rule will result in immediate termination and prosecution to the fullest extent of the law.

Organization Funds and Other Assets

Employees who have access to Organization funds in any form must follow the prescribed procedures for recording, handling and protecting money as detailed in the Organization's instructional manuals or other explanatory materials, or both. The Organization imposes strict standards to prevent fraud and dishonesty. If employees become aware of any evidence of fraud and dishonesty, they should immediately advise their superior or the Law Department so that the Organization can promptly investigate further.

When an employee's position requires spending Organization funds or incurring any reimbursable personal expenses, that individual must use good judgment on the Organization's behalf to ensure that good value is received for every expenditure.

Organization funds and all other assets of the Organization are for Organization purposes only and not for personal benefit. This includes the personal use of organizational assets such as computers.

Figure 2-2. *(continued)*

Organization Records and Communications

Accurate and reliable records of many kinds are necessary to meet the Organization's legal and financial obligations and to manage the affairs of the Organization. The Organization's books and records must reflect in an accurate and timely manner all business transactions. The employees responsible for accounting and record-keeping must fully disclose and record all assets, liabilities, or both, and must exercise diligence in enforcing these requirements.

Employees must not make or engage in any false record or communication of any kind, whether internal or external, including but not limited to—

- False expense, attendance, production, financial or similar reports and statements
- False advertising, deceptive marketing practices, or other misleading representations

Dealing With Outside People and Organizations

Employees must take care to separate their personal roles from their Organization positions when communicating on matters not involving Organization business. Employees must not use organization identification, stationery, supplies and equipment for personal or political matters.

When communicating publicly on matters that involve Organization business, employees must not presume to speak for the Organization on any topic, unless they are certain that the views they express are those of the Organization, and it is the Organization's desire that such views be publicly disseminated.

When dealing with anyone outside the Organization, including public officials, employees must take care not to compromise the integrity or damage the reputation of either the Organization, or any outside individual, business, or government body.

Prompt Communications

In all matters relevant to customers, suppliers, government authorities, the public and others in the Organization, all employees must make every effort to achieve complete, accurate and timely communications—responding promptly and courteously to all proper requests for information and to all complaints.

Privacy and Confidentiality

When handling financial and personal information about customers or others with whom the Organization has dealings, observe the following principles:

1. Collect, use, and retain only the personal information necessary for the Organization's business. Whenever possible, obtain any relevant information directly from the person concerned. Use only reputable and reliable sources to supplement this information.

(continued)

Figure 2-2. *(continued)*

2. Retain information only for as long as necessary or as required by law. Protect the physical security of this information.
3. Limit internal access to personal information to those with a legitimate business reason for seeking that information. Only use personal information for the purposes for which it was originally obtained. Obtain the consent of the person concerned before externally disclosing any personal information, unless legal process or contractual obligation provides otherwise.

When designing your program, implementation strategy and training, remember the following bit of wisdom:

> *Give a person a fish and he or she will be able to eat today. Teach a person to fish and he or she will be able to eat for a lifetime.*

If you try to create a rule for every ethical dilemma, your people will focus on how to fit their decisions to the rules. On this premise, if there is no rule, there is no problem. If you train your people to make ethical decisions for themselves, however, they will focus on doing just that.

Training and Communication

After writing your organization's code of ethics and business conduct, ask everyone to read it and have them confirm in writing that they have done so and understood the content. Keep a record of this acknowledgment.

You should consider seminar training for all employees and agents. The training doesn't have to be long and complicated. Use the KISS (Keep It Simple Stupid) method to develop your ethics curriculum. Instead of giving them rules, give them tools. These tools can be as simple as a list of broad principles to follow and questions to ask when making decisions.

In *Policies and Persons: A Case Book in Business Ethics,* John B. Mathews and coauthors suggest the following tools.

1. Avoid harming others.
2. Prevent harm to others.
3. Respect the rights of others.
4. Do not lie or cheat.
5. Keep promises and contracts.
6. Obey the law.
7. Help those in need.
8. Be fair.

So, when a considered action may raise serious ethical questions, try applying the generalized criteria. For example, you can use the guidelines above and ask yourself the following specific questions.

1. Does the considered action violate any of the following?:
   —A criminal law
   —A civil law
   —A company policy
   —A professional code
   —An industry code
   —My personal values
2. Is the action fair, just, and equitable to all parties?
3. Does the action serve the common good and the public's interest?
4. Does it provide the greatest good for the greatest number?
5. Does it do the least harm to the greatest number?
6. Does it cost more than its social benefits?
7. Would you like it if it were done to you (known as "The Golden Rule")?
8. Would an ethical role model (for example, your parent, priest, or minister) approve of this act?

Enforcement

As discussed in chapter 1, an effective prevention strategy demands there be some adverse consequences when an employee is caught committing fraud (for example, dismissal of the employee and the pressing of charges). Similarly, there also must be some adverse consequences—commensurate with the severity of the breach—when an employee contravenes an organization's stated policies, and in particular its code of ethics and business conduct. For severe breaches, or for repeat offenders, dismissal may be an appropriate consequence and the organization's policies should so state.

To ensure that all employees are aware of their responsibilities, organizations should require that the staff sign an annual declaration stating they are aware of the company's code of ethics and business conduct policies, and confirming they have complied in the past and will continue to do so.

Employee Hiring and Employee Relations

Ultimately, the employees, not the organization's policies, create a good ethical climate. Employee hiring practices and employee relations are therefore important fraud prevention variables. The Ethical Environment Checklist (at the end of this chapter) provides a fairly comprehensive list of the factors to consider.

Generally, organizations face a balancing act. On the one hand, they must minimize the risk of fraud and be cost-effective in employee remuneration. On the other hand, they must promote an open environment in which employee morale and creativity flourish, while employees feel rewarded for their efforts. Tipping the scale too far to one side or the other can lead to problems, or reduce the competitiveness of an organization, or both. Organizations can achieve success at a point somewhere in between and only through the good judgment of management.

2.1.4 Ethics and Information Technology

The ever-accelerating information revolution—particularly during the latter half of the twentieth century—has raised special ethical issues. In particular, makers, distributors, owners, managers, and users of information resources have ethical responsibilities for the products and services that they create, own, sell, manage, and use. The ethical issues raised by information technology include the following:

- Privacy
- Piracy
- Safety and health
- Data security
- Data integrity
- Competence
- Honesty
- Loyalty
- Fairness

Privacy

A myriad of both private-and public-sector organizations collect data for a wide variety of purposes. The U.S. government alone has gathered and stored four billion records on individuals. The development of database management software for personal computers has extended these capabilities to anyone with a few hundred dollars. Although databases have grown explosively, controls over access and disclosure of confidential data have not kept pace. Unauthorized access to databases and disclosure of confidential information contained therein are commonplace.

There are legal constraints on the improper collection and dissemination of personal data in the United States and Canada, embodied in their respective Constitutions, Supreme Court decisions, tort law, and in federal and state privacy and consumer rights enactment. However, these laws and rulings are not sufficiently clear to reach consensus. For example, on the question of access to personal history databases versus an individual's right of privacy, an ethicist might ask the following.

- Who is collecting the data?
- For what use are the data being collected?
- How, to whom, and for what purpose will the data be disseminated?
- How well protected is that data against unauthorized access and disclosure?
- How accurate, complete, and timely are the data?
- What degrees of confidentiality should be accorded to such disparate data as medical, psychiatric, credit, employment, school and criminal records?

If medical records were considered the most confidential of the lot, the ethical standard for the care accorded such data would be higher; that is, medical records should be gathered, stored, and disseminated with great care and caution.

Piracy

Software piracy signifies that the creative work of another has been used or duplicated without permission or payment of royalty, or both. The definition assumes that the software's creator has complied adequately with the legal requirements of the federal copyright law. Therefore, the software pirate commits an act of infringement and may be civilly sued for damages, criminally prosecuted, or both.

Software piracy is probably the most common breach of ethics in the field of information technology. For each software program sold, developers claim that another two to five copies are bootlegged. The lost royalties of developers are staggering. Some thieves rationalize that software prices are too high and that the developers are large and will not miss the lost royalties. In reality, the software industry has become increasingly competitive and losses to piracy can have a serious impact on a company's viability. Moreover, even the largest and most profitable developers have a right to seek a fair price and return for their development efforts, the costs incurred and the risks taken.

Safety and Health

The widespread use of computers in today's information-driven economy has contributed to and in some instances created, unique safety issues that can be divided into the following two distinct categories:

1. Accidents resulting from the use of computer-controlled systems
2. Occupational health and safety problems for users caused by long-term or improper use of computers, or both

Computer-controlled systems safety issues—The accelerated pace of technological change in this century has resulted in an exponential increase in new industries with many innovative products and processes. Dangerous substances and sensitive information are being handled on an unparalleled scale. New systems are being built—using computers to control them—that have the capacity to cause extensive destruction of life and the environment. A single accident could be catastrophic. Computers now control most safety-critical devices and they often replace traditional hardware safety interlocks and protection systems. Even when hardware protection devices are retained, software is often used to control them. Because of the explosive increase in the use of, and reliance on computers, methods to ensure the safety of computer-controlled systems have not always kept pace with the development of these very systems. Ethicists recognize there is a serious danger of overreliance on the accuracy of computer outputs and databases. The nonoccurrence of particular types of accidents in the past is no guarantee that they will not take place in the future. Software and hardware developers and information technology professionals alike must recognize their moral and ethical responsibilities. We can't wait to learn from experience, but must attempt to anticipate and prevent accidents before they occur.

Computer-related safety and health issues—Today's computer operators, particularly heavy users, may develop problems caused by the repetitive motions used daily in operating their machines. The most common problem is repetitive stress injury (RSI), in which workers experience moderate to severe pain in the muscles and joints of the hands, wrists, arms, shoulders, neck and back. RSI can be caused by carpal tunnel syndrome (CTS), irritation of the nerves leading to the fingers due to the prolonged use of a keyboard while the body is in an unnatural or strained position. RSI can be completely incapacitating, sometimes requiring surgery if not treated early. According to Patrick G. McKeown in his text, *Living With Computers*, these injuries are epidemic in computer-related jobs; RSI constitutes more than 60 percent of work injuries and costs employers $20 billion annually. Other health-related problems involve radiation emissions from the monitor and eyestrain from watching the screen for long periods of time without proper lighting or screen glare protection, as well as noise-induced problems caused by the pervasive low-level noise in today's computer environment.

Because of the enormous costs resulting from worker's health and safety issues, many organizations are opting for ergonomically designed work environments. Ergonomics, or human factor engineering, is the science of designing equipment for the workplace to keep employees safe and healthy while they work, which usually results in fewer physical complaints, higher employee morale and increased productivity. An ergonomically designed work area considers the following factors:

- The height and position of the monitor
- The height and angle of the keyboard
- A fully adjustable chair that provides lower back and adjustable arm support and height adjustment capabilities
- A keyboard that allows users to work with their hands in a natural position
- A mouse designed for either a left- or right-handed user with wrist support
- An anti-glare monitor screen
- Noise reduction measures
- Proper indirect and task lighting
- Adequate ventilation

In addition, employers should emphasize the proper use of equipment, encourage regular breaks, and provide stress reduction training for employees to further minimize the risk factors related to RSI and related injuries. In an ethical environment management is sensitive to the well-being of regular employees and applies the same principles to part-time workers and support staff.

Data Security

The protection of personal information from unauthorized access, disclosure, and duplication obligates a database owner to—

- Formulate and enforce standards for the proper use of the data.
- Communicate to, educate, and train users about their responsibility for protecting such information.
- Plan for likely contingencies.
- Establish adequate security controls.
- Monitor control exceptions.

Data Integrity

An incorrectly entered arrest report, credit report, insurance rejection, debt default, or lab test can cause great emotional and financial damage. Yet the error rates of databases with such sensitive information are often higher than the standards of quality set by the original designers of these systems. Accuracy, timeliness, completeness, and relevance are what give information its value. In particular, creators of personal history databases have a special obligation to compile and process such data accurately and to protect it from the prying eyes of snoops, browsers, and hackers.

Today people can collect, process and disseminate information at a high speed. If information is irrelevant to the needs of users or is flawed in logic, assumptions or conclusions, relying on such specious data can cause catastrophic damage. Therefore, quality begins with clear objectives, exacting designs, flawless development and proper training of users. People and organizations involved in software development and database design are obliged to make products that are fit for their intended uses and have no fundamental defects.

Competence

The field of information technology is notable for its fast growth and complexity, and the sweeping social, economic, and political changes it has wrought. At times, change seems overwhelming. Skills and products become obsolete overnight. Companies must invest large sums of money in research and product development.

In the race to get new products out of the labs and into the market, people often compromise quality, safety and security. New products might contain design flaws, software errors, bugs and glitches, and other impediments to proper functioning. These impediments can be costly to uninformed and unsophisticated users. Makers and providers of information technology products—both hardware and software—must take great care and caution in their work to avoid damage or interruption of service to their users. Providers of information technology should seek the most competent people available for sensitive design and product development projects. They should also create an ethical climate in their firms and foster responsible behavior among all employees.

Honesty

Makers, sellers, dealers, distributors, and installers of information technology products—like all other business people—must be honest in their dealings with one another. All parties should use truthful representations, nondeceptive advertising, and accurate labeling, as well as fulfill contract requirements.

Loyalty

The information technology industry is large, complex, fast changing, and highly competitive. Some information products—such as chips and PCs—have become commodities. The relationship between buyers and sellers is changing from one in which mutual trust, confidence, and faith give way to arms-length transactions. Sellers attract buyers on the basis of price alone. The service-after-sale element is forgotten.

These same industry dynamics have also changed the relationship between employers and employees. Loyalty is supposed to be a two-way street. In today's competitive environment, some high-tech, high-talent employees are loyal only to their paychecks thereby blurring obligations between employers and employees, sellers and buyers, and manufacturers and suppliers.

Fairness

Normally people conduct business on the basis of mutual faith and trust. You cannot, however, provide for all contingencies in a formal contract. The writing and execution of a detailed contract would take too long, thus frustrating the objectives of both parties.

Assuming business ethics are a matter of mutual rights and obligations of the transacting parties implies that fairness is the rule by which we measure whether a transaction is right or wrong. In theory, both parties have equal bargaining power in a commercial transaction. Therefore, ethics should leave the parties to their own negotiations. Often in the information industry, both parties are not of equal size, competence, skill, knowledge or experience. In these circumstances, fairness may mean that the more powerful of the two has an added measure of obligation. The English common law treated buyers and sellers as equally competent to transact business. Yet in the modern era the notion of *caveat emptor* (let the buyer beware) has been diluted. Sellers with superior knowledge, skills, and resources must be most forthcoming. Fairness may no longer be a 50-50 proposition. Fairness depends on the relationship between the parties, their relative power positions, and the context of the business transaction.

2.2 Ethical Environment Checklist

CPAs can use table 2.1, Ethical Environment Checklist to help promote an ethical environment in their organizations and in those of their clients. ***No*** answers may require investigation and follow-up, the results of which should be documented. Use the *Ref* column to cross-reference the checklist to appropriate work papers.

Some sections in this comprehensive checklist may not be applicable or appropriate in certain instances. For example, most organizations will not conduct the entire employee screening procedures described in section 4 of the checklist. This checklist is intended for general guidance and information only. Use of this checklist does not guarantee the prevention of fraud. If fraud prevention is an especially vital concern or if fraud is suspected, consider seeking the advice of a knowledgeable fraud practitioner.

TABLE 2.1 ETHICAL ENVIRONMENT CHECKLIST

Ethical Environment Checklist	Yes	No	NA	Ref
1. Organizational Approach to Ethics				
a. Does the organization have a Mission Statement that emphasizes respect for the law, ethics, and ethical conduct?	☐	☐	☐	___
b. Does the organization have a written and enforced Code of Ethics?	☐	☐	☐	___
c. If the organization or its employees are subject to outside ethical standards and rules (e.g., industry or professional), does the organization's code refer to and emphasize their importance?	☐	☐	☐	___
d. Does the organization have—				
• Internal auditors?	☐	☐	☐	___
• Electronic data processing (EDP) auditors?	☐	☐	☐	___
• At least one Data-Security Officer or Administrator?	☐	☐	☐	___
• A Corporate-Security or Loss-Prevention Unit?	☐	☐	☐	___
• An investigative staff?	☐	☐	☐	___
e. Does the organization, as a matter of written policy, refer incidents of employee crimes on the job to police or prosecutorial authorities?	☐	☐	☐	___
f. If the organization has experienced fraud in the past five years, has management established the causes and taken remedial action for any of the following:				
• A substantial inventory shortage corporate-wide	☐	☐	☐	___
• A substantial inventory shortage in a major operating division	☐	☐	☐	___
• A major embezzlement involving a loss of more than $10,000	☐	☐	☐	___
• A successful penetration of the main office computers by outsiders	☐	☐	☐	___
• An accounts payable, accounts receivable, payroll, or benefit claim fraud of any amount	☐	☐	☐	___
• A commercial bribery of purchasing or other personnel	☐	☐	☐	___
2. Situational Approach to Ethics				
a. Are ethical considerations a critical element in corporate policies, tactics, and decision-making?	☐	☐	☐	___
b. Is there a specific framework—especially for important and difficult corporate decisions or actions—for addressing the ethical element, such as a series of questions like those set out in item *2c* (below)?	☐	☐	☐	___

(continued)

TABLE 2.1 *(continued)*

Ethical Environment Checklist	Yes	No	NA	Ref
c. Does the organization, when contemplating actions or decisions that may raise ethical concerns, consider the following:				
• Does the action violate any law or code to which the organization is subject?	☐	☐	☐	___
• Is the action fair, just and equitable to all the parties involved?	☐	☐	☐	___
• Does the action serve the common good and the public's interest (for example, does it: (i) provide the greatest good for the greatest number, (ii) do the least harm to the greatest number, and (iii) yield social benefits that exceed the cost)?	☐	☐	☐	___
• Would an ethical purist or role model (for example, the stereotypical good parent, priest or minister) approve of the act?	☐	☐	☐	___
3. Policy Approach to Ethics				
a. Does management set the right tone for employees and demonstrate the organization's commitment to ethical conduct (for example, by regularly referring to the organization's code of ethics in policy meetings and communications)?	☐	☐	☐	___
b. Do the organization's policies in all activities, communications, and transactions reflect a commitment to the following:				
• Honesty and integrity	☐	☐	☐	___
• Competence and due care	☐	☐	☐	___
• Commitment to excellence	☐	☐	☐	___
• Fair and prompt dealings	☐	☐	☐	___
• Respect for privacy and confidentiality	☐	☐	☐	___
c. Does the organization have written policies that restrict or prohibit the following:				
• Engaging in outside employment (moonlighting)	☐	☐	☐	___
• Engaging in conflicts of interest	☐	☐	☐	___
• Accepting gratuities, expensive gifts or lavish entertainments from vendors, contractors and suppliers	☐	☐	☐	___
• Compromising or bribing customers	☐	☐	☐	___

TABLE 2.1 *(continued)*

Ethical Environment Checklist	**Yes**	**No**	**NA**	**Ref**
• Engaging in false advertising and deceptive marketing practices	☐	☐	☐	____
• Disclosing company trade secrets to unauthorized persons	☐	☐	☐	____
• Fixing prices with competitors	☐	☐	☐	____
• Gambling on the job	☐	☐	☐	____
• Abusing drugs or alcohol, or both	☐	☐	☐	____
• Fighting on the job	☐	☐	☐	____
• Stealing company property, including personal use of company property (for example, computer time)	☐	☐	☐	____
• Destroying company property	☐	☐	☐	____
• Falsifying time or attendance reports	☐	☐	☐	____
• Falsifying production reports	☐	☐	☐	____
• Falsifying personal data on a job application	☐	☐	☐	____
• Falsifying or forging accounting records	☐	☐	☐	____
• Destroying accounting records	☐	☐	☐	____
• Falsifying expense accounts	☐	☐	☐	____
• Allowing unauthorized persons access to confidential records (for example, payroll and personnel records, customer and vendor lists, research results, product and marketing plans)	☐	☐	☐	____
• Allowing unauthorized persons access to company buildings or critical work areas	☐	☐	☐	____
• Loaning company building access identification cards, badges or door keys to unauthorized persons	☐	☐	☐	____
• Disclosing computer log-on codes or passwords to unauthorized persons	☐	☐	☐	____
• Allowing unauthorized persons use of computer terminals	☐	☐	☐	____
4. Ethics and Human Resources				
a. To the extent necessary, when considering an applicant and depending on the importance and sensitivity of the position, does the organization perform reference checks, background inquiries or investigations, or any combination thereof, to confirm the applicant's—				
• Identity	☐	☐	☐	____
• Educational achievements	☐	☐	☐	____

(continued)

TABLE 2.1 *(continued)*

Ethical Environment Checklist	Yes	No	NA	Ref
• Credit standing	☐	☐	☐	___
• Satisfactory past employment history	☐	☐	☐	___
• Absence of criminal convictions (including name or fingerprint checks, or both)	☐	☐	☐	___
• Reputation	☐	☐	☐	___
• Character	☐	☐	☐	___
b. Especially for very sensitive positions (for example, those affecting public safety, the custodianship of large amounts of cash or securities, the secrecy of important information), and to the extent allowed by law, does the organization administer any of the following to employees and prospective employees:				
• Polygraphs	☐	☐	☐	___
• Paper and pencil honesty tests	☐	☐	☐	___
• Voice stress analyses	☐	☐	☐	___
• Handwriting analyses	☐	☐	☐	___
• Intelligence tests	☐	☐	☐	___
• Psychological diagnostic tests	☐	☐	☐	___
• Drug tests	☐	☐	☐	___
c. Does the organization conduct or provide (or both) any of the following:				
• Security orientation training for new hires	☐	☐	☐	___
• Ongoing security awareness training programs for all employees	☐	☐	☐	___
• Written rules of employee conduct to all employees	☐	☐	☐	___
• Annual, signed employee declarations acknowledging awareness of the company's code of conduct, and past and future adherence to it	☐	☐	☐	___
• Hearings for employees charged with punishable offenses	☐	☐	☐	___
• Employee representation at such hearings	☐	☐	☐	___
d. Does the organization use or provide any of the following:				
• Job descriptions	☐	☐	☐	___
• Organization charts	☐	☐	☐	___
• Performance standards	☐	☐	☐	___
• Performance appraisals	☐	☐	☐	___

TABLE 2.1 *(continued)*

Ethical Environment Checklist	Yes	No	NA	Ref
• Coaching and counseling of employees whose work is unsatisfactory	☐	☐	☐	___
• Counseling of employees with drug abuse problems	☐	☐	☐	___
• Technical training programs	☐	☐	☐	___
• Human resource development programs	☐	☐	☐	___
• Tuition reimbursement	☐	☐	☐	___
• Time off for study	☐	☐	☐	___
• Time off for family emergencies	☐	☐	☐	___
• Employee involvement programs	☐	☐	☐	___
• Job enlargement, enrichment or rotation programs	☐	☐	☐	___
• Exit interviews for departing employees	☐	☐	☐	___
e. Does the organization compare favorably or at least equally with other firms in its industry, or areas of operations, or both, with respect to any of the following:				
• Salaries	☐	☐	☐	___
• Fringe benefits	☐	☐	☐	___
• Blue-collar turnover	☐	☐	☐	___
• White-collar turnover	☐	☐	☐	___
• Absenteeism	☐	☐	☐	___
• Employee firings	☐	☐	☐	___
• Promotions from within the company	☐	☐	☐	___
• Ability to recruit new employees	☐	☐	☐	___
• Skills of its employees	☐	☐	☐	___
• Educational level of employees	☐	☐	☐	___
• Employee attitudes toward their work	☐	☐	☐	___
• Employee loyalty	☐	☐	☐	___
5. Ethics and Information Technology				
a. Does the organization's code of conduct specifically address the importance of using information technology (especially computers) in an ethical manner?	☐	☐	☐	___
b. Are the following specific ethical concerns relating to information technology adequately addressed in the organization's code of conduct and in its policies:				

(continued)

TABLE 2.1 *(continued)*

Ethical Environment Checklist	Yes	No	NA	Ref
• Privacy of information (for example, information related to employees, customers or clients)	☐	☐	☐	___
• Prohibition of software piracy	☐	☐	☐	___
• Safety and health (for example, ergonomically sound computer workstations)	☐	☐	☐	___
• Quality standards for information technologies and the information they process (for example, accuracy, integrity, security)	☐	☐	☐	___
• Relationship of technology and human resources (for example, communication with employees concerning technological change, adequate training)	☐	☐	☐	___

CHAPTER 3:

Risk Financing and Fidelity Insurance

CHAPTER 3:

Risk Financing and Fidelity Insurance

3.1 THE CONCEPT OF RISK FINANCING

The risk of loss due to fraud and other forms of dishonesty can never be completely eliminated. Organizations can finance the potential loss either by purchasing fidelity insurance coverage or by self-insuring the risk, that is, absorbing out of one's own pocket any losses incurred. Experts recommend giving serious consideration to purchasing insurance in situations with significant risk or potential loss. In reality, however, many organizations choose the self-insurance default because they either fail to assess the risk and its financial impact or they are simply unfamiliar with fidelity insurance.

Most individuals and businesses would never—or at least should never—consider self-insurance as a viable option in the case of potentially catastrophic risk. Examples of insuring against potentially catastrophic risks include life and disability insurance for breadwinners supporting families, fire insurance for homeowners, and liability insurance for doctors and automobile owners. In some cases, a statute or contractual agreement may mandate insurance; for example, a mortgage agreement may require fire insurance. The risk of catastrophic loss due to fraud merits serious consideration for the purchase of fidelity coverage.

This chapter reviews the kinds of available "dishonesty" insurance including the issues typically addressed in a policy, policy exemptions and the duties of the insured. The remainder of the chapter provides some insights into preparing an employee dishonesty claim.

3.2 DISHONESTY INSURANCE

3.2.1 Overview

Insurance coverage for dishonest acts is known by many names, including fidelity insurance, commercial crime coverage, blanket bonds and 3D policies (Dishonesty, Destruction and Disappearance). The desired coverage can be written in standard bond or policy language, as a rider to other insurance policies, or in a manuscript format, that is, written for a specific company or organization.

For certain industries there are standard policy-bond forms. For example, there are standard forms for financial institutions such as banks, brokerages and insurance companies. For other industries, including manufacturing, health care, retailing, transportation or service providers, dishonesty coverage is more generic. Regardless of name, the policies generally follow a similar format. This Handbook uses the term *commercial crime policy* to refer to dishonesty coverage except in discussions of other, specific kinds of coverage.

3.2.2 The Policy Provisions

When considering the purchase of dishonesty coverage, you should understand what is and what is not covered under the policy. Generally, you can acquire an understanding from the four major policy provisions:

1. *Insuring agreements* that describe what the policy covers
2. *Definitions* that provide specificity of terms of coverage and effectively limit the scope for interpretation of coverage
3. *Exclusions* that enumerate what the policy does not cover
4. *Duties of the insured* that specify what the insured must do to receive indemnity under a policy

3.2.3 Coverage in Insuring Agreements

The first sections of a policy, usually called *insuring agreements*, specify what types of losses are covered. Typically, the insuring agreements (and riders when necessary) cover—

- Employee dishonesty
- Loss Inside the Premises
- Loss Outside the Premises
- Money Order Fraud and Counterfeit Paper
- Depositor Forgery

Employee Dishonesty

The generally used employee dishonesty Blanket Coverage Form Insuring Agreement (CR 00 01) is shown in figure 3-1. You should note that coverage applies only to loss of "covered property."

Covered property is defined very narrowly in the insuring agreement and, in addition, the terms used in that agreement are also subject to further specific definitions. Therefore, when considering filing a claim, one of the first questions that you should answer is whether covered property was lost. Also, you should make sure to tailor your coverage to your organization's specific industry and needs, and to include the kinds of risks your organization may encounter.

Insuring Agreements and riders are also available to cover losses caused by non-employees. These include the following:

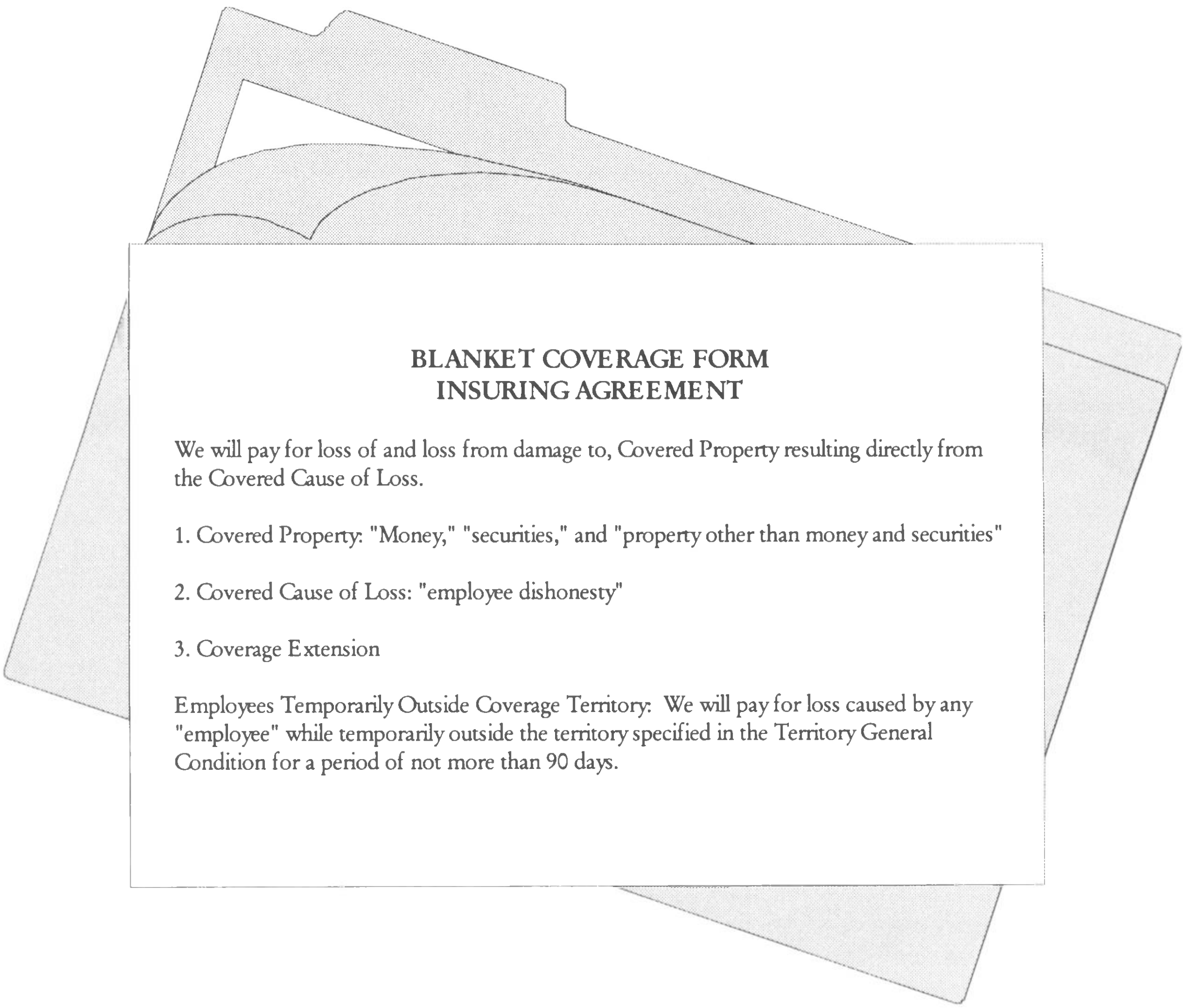
Loss Inside the Premises

Organizations can insure against loss inside the premises, which is defined in most agreements and riders as "Losses of money and securities by the actual destruction, disappearance or wrongful abstraction . . . within the premises . . . or banking premises . . . . Including loss resulting from safe burglary or robbery with the premises . . . ."

Loss Outside the Premises

Organizations can insure against loss outside the premises, which is defined in most agreements and riders as a "Loss of money and securities and other property . . . while being conveyed by messenger . . . or armored car company."

Figure 3-1. Blanket Coverage Form Insuring Agreement (CR 00 01)



BLANKET COVERAGE FORM
INSURING AGREEMENT

We will pay for loss of and loss from damage to, Covered Property resulting directly from the Covered Cause of Loss.

1. Covered Property: "Money," "securities," and "property other than money and securities"

2. Covered Cause of Loss: "employee dishonesty"

3. Coverage Extension

Employees Temporarily Outside Coverage Territory: We will pay for loss caused by any "employee" while temporarily outside the territory specified in the Territory General Condition for a period of not more than 90 days.

Money Order Fraud and Counterfeit Paper

Organizations can insure against money order fraud and counterfeit paper, which is defined in most agreements and riders as "Loss due to the acceptance in good faith, in exchange for merchandise, money . . . in the normal course of business of counterfeit currency, money orders, etc., through the Insured bank account . . . ."

Depositor Forgery

Organizations can insure against depositor forgery, which is defined in most agreements and riders as "Loss as a result of the Insured having someone process forged checks, money orders, etc., through the Insured bank account . . . ."

3.2.4 Riders

Remember you can add riders to the standard policy coverage to provide for the unique areas of risk not otherwise included. Some riders that you should consider include coverage for loss from:

- Unauthorized electronic transfers
- Pension plan frauds
- Credit card forgeries
- Computer frauds
- Unauthorized use of telephone services

3.3 Important Clauses in Dishonesty Policies

3.3.1 Policy Definitions

Other policy provisions include definitions of the terms used in the insuring agreements. Usually, the definitions are used to limit the scope for interpreting the terms of coverage. For example, the employee dishonesty insuring agreement describes a covered loss as one resulting from *employee dishonesty.* This term and the term *employee,* on which it relies, are further defined to provide specific qualifications of coverage as to cause. Figure 3-2 contains a typical policy definition of employee dishonesty.

For coverage to apply, the first requirement is that an *employee* must commit the covered act. If the perpetrator were not an employee, coverage would not apply. This requirement makes it important to determine the identity of the perpetrator(s).

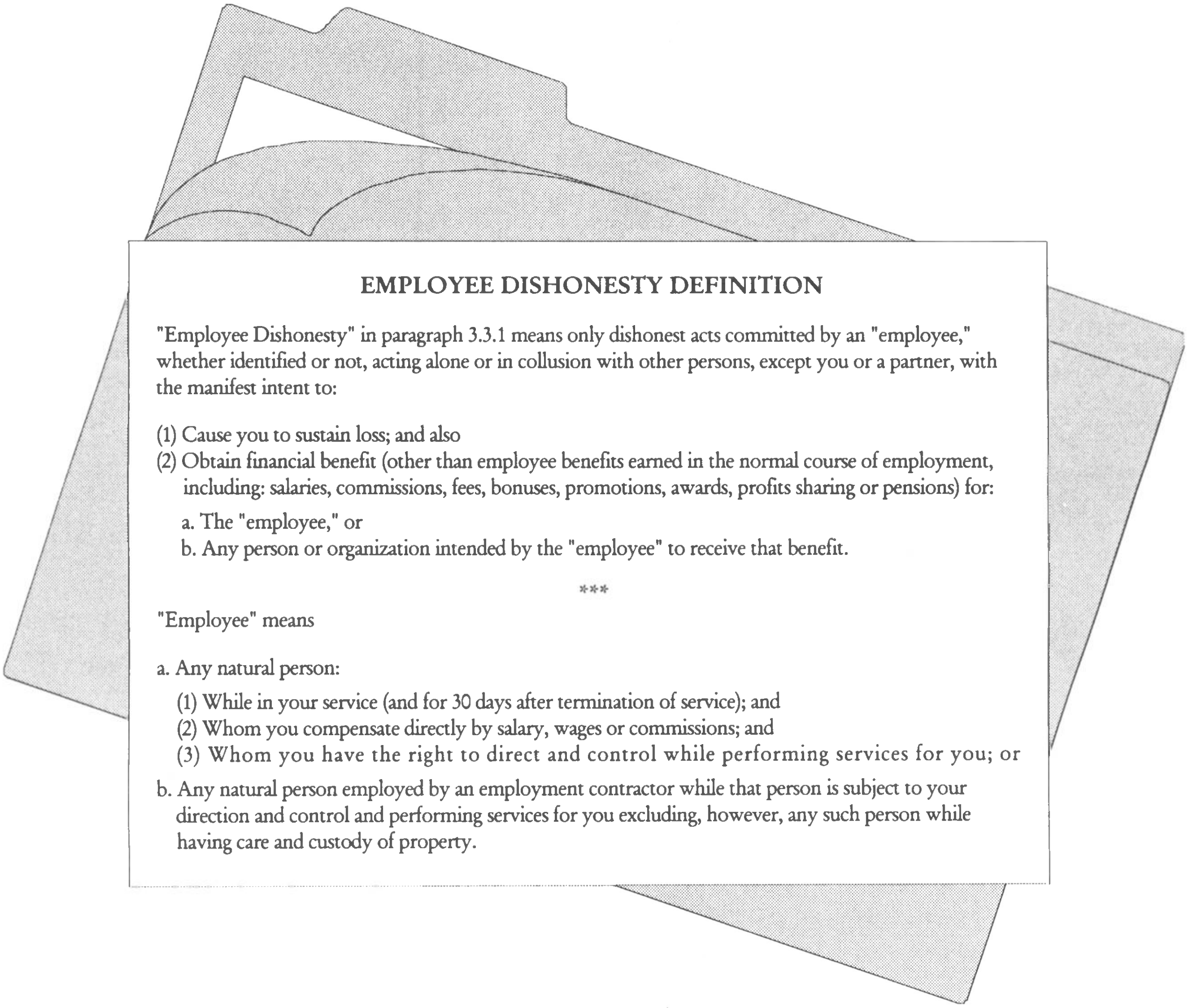
While the policy language specifically defines the term *employee,* you can request endorsements to alter the definition and to expand coverage of certain other parties (for example, volunteer workers and designated agents) as employees.

Because a policy provides a specific definition of dishonesty, it is important for you to ascertain—

1. That the employee committed the act with the *manifest intent* to cause the insured to incur a loss, and
2. That the employee or some intended third party received a benefit. Few other provisions in a policy have resulted in as much litigation as this one, particularly concerning the meaning of *manifest intent.*

Unfortunately, there is no consensus among jurisdictions on the interpretation of *manifest intent*; rather, there is a broad spectrum of interpretations. Some courts have found this term to apply only to those situations where the employee has the intent to gain a benefit for someone at the expense of the insured. Other courts have found a broader meaning affording coverage for situations in which the employee acted with such disregard for the insured that the loss was a substantial certainty. In one case involving the definition of the term a court ruled, "Such a person is deemed to intend the natural and probable consequences of his acts."

Figure 3-2. Typical Policy Definition of Employee Dishonesty



EMPLOYEE DISHONESTY DEFINITION

"Employee Dishonesty" in paragraph 3.3.1 means only dishonest acts committed by an "employee," whether identified or not, acting alone or in collusion with other persons, except you or a partner, with the manifest intent to:

(1) Cause you to sustain loss; and also
(2) Obtain financial benefit (other than employee benefits earned in the normal course of employment, including: salaries, commissions, fees, bonuses, promotions, awards, profits sharing or pensions) for:
   a. The "employee," or
   b. Any person or organization intended by the "employee" to receive that benefit.

***

"Employee" means

a. Any natural person:
   (1) While in your service (and for 30 days after termination of service); and
   (2) Whom you compensate directly by salary, wages or commissions; and
   (3) Whom you have the right to direct and control while performing services for you; or
b. Any natural person employed by an employment contractor while that person is subject to your direction and control and performing services for you excluding, however, any such person while having care and custody of property.

Consequently, an insured should not necessarily give up on a claim just because the insurer believes the dishonest individual did not possess the requisite *manifest intent.* Before challenging a claim denial, legal counsel should be retained to conduct research to discover how the applicable jurisdiction interprets this language. Then if favorable case law is found, you can approach the insurer seeking a reversal of the claim denial.

3.3.2 Policy Exclusions

The policy describes the covered losses and the specific exclusions for losses that it will not cover. Because insurers tailor each policy with its own list of exclusions, you should read and understand the terms before purchasing the coverage.

Although we won't explore the legal implications of policy provisions, you should consider the practical problems arising from the exclusions both when purchasing the coverage and when preparing a proof of loss. Even though the specific exclusions can vary, here are some examples of typical exclusions found in many standard policies:

Indirect Losses

Commercial crime policies specifically exclude indirect and consequential losses. It is generally accepted that this exclusion's original intent was to limit the coverage to direct losses, thus, excluding consequential losses, such as lost profits, lost business opportunities, or lost interest on stolen funds. While this exclusion's intent may seem to be clear, judicial interpretations remain inconsistent. Clearly, you should discuss this issue with legal counsel, who can interpret the relevant case law in the applicable jurisdiction(s).

An indirect loss may involve the costs incurred in establishing the insured's claim. Again, this provision excludes from coverage the costs of investigating and quantifying a claim. In today's market, you can purchase coverage for the costs of establishing a claim. Some carriers write policies that cover all, or a stated amount, of an investigation's costs, while others write policies under which the costs are shared between the insured and the carrier. Of course, you should evaluate the cost of purchasing this coverage in light of the potential cost of any investigation. The indirect loss policy provision is excerpted in figure 3-3.

Inventory Loss

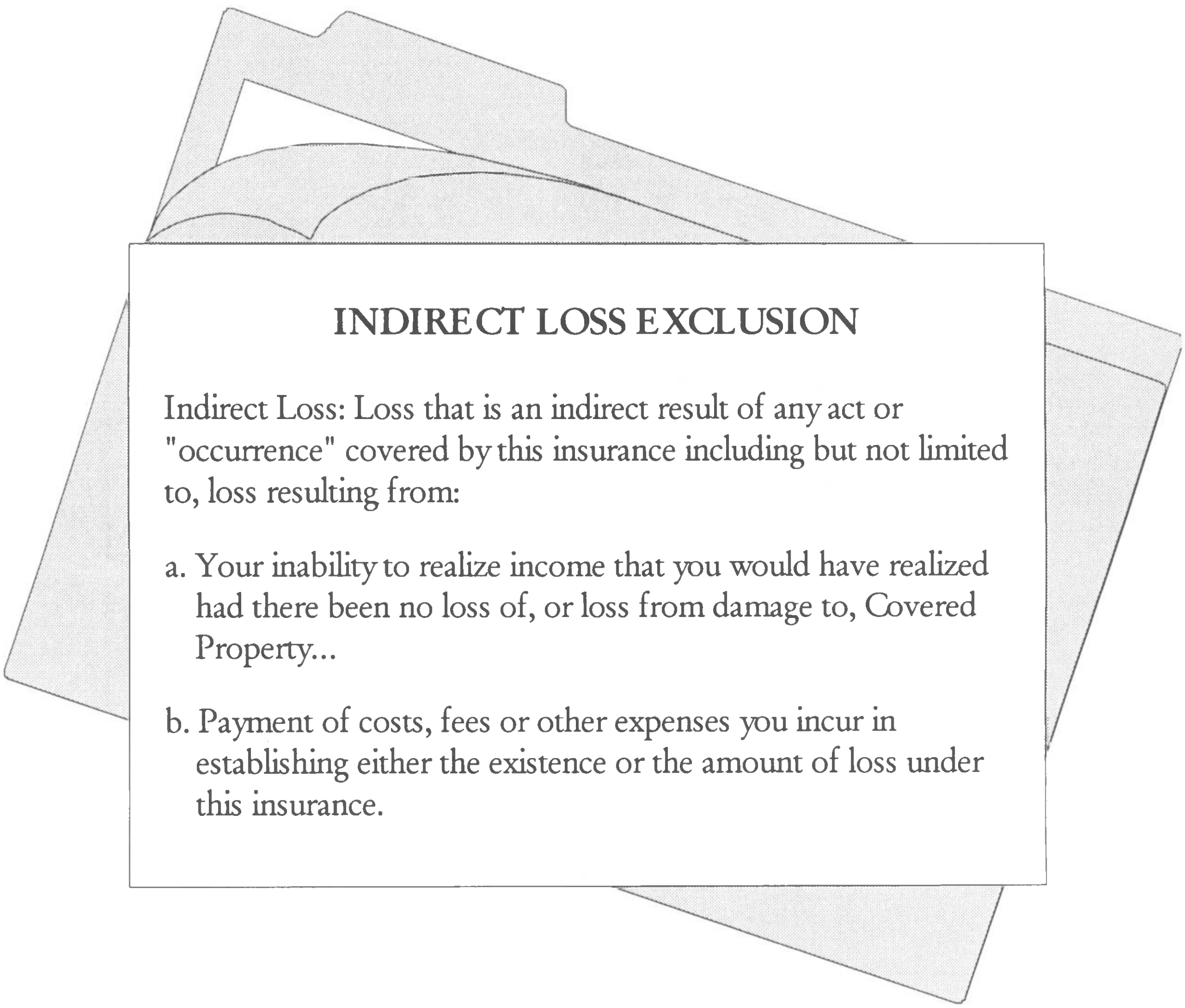
The inventory loss exclusion addresses losses of inventory when the insured may catch dishonest employees with "the goods," or the employees may confess their dishonesty, but the insured cannot prove the extent of the dishonest acts and the resulting losses. See figure 3-4 for an example of a standard inventory loss exclusion.

Under this exclusion, an insurer will not accept a shortage of inventory on a comparison of book to physical quantities as proof of dishonesty nor as verification of the quantum of loss sustained. Similarly, the insurer will not consider a reduction in profits as proof of dishonesty or loss because there can be other plausible explanations for either an inventory shortage or a reduction in profits.

Thieves normally keep few, if any, records, and their veracity, at best, is questionable. Often, dishonest employees purposely understate, in their confessions, the extent of the losses in the hopes of avoiding not only prosecution but also any subsequent requirement to make restitution. Conversely, dishonest employees may overestimate losses in an effort to appease their employers by supporting a claim for a large insurance recovery. Simply stated, most dishonest employees do not know how much they have actually stolen.

For example, an employee of an auto parts dealer is caught with a trunk full of stolen automobile parts. When confronted, the employee confesses to stealing parts for four years but doesn't have the slightest idea of how much he actually took. In this situation, an insured instinctively presents a proof of loss based on an inventory computation. Essentially, this methodology attempts to blame all shortages, including those in the normal inventory process, on the dishonest employee. Therefore, if the insured compares the physical inventory available with the inventory records and discovers a shortage of $400,000 in automobile parts, the insured may attempt to claim this amount.

Figure 3-3. Indirect Loss Policy Provision



INDIRECT LOSS EXCLUSION

Indirect Loss: Loss that is an indirect result of any act or "occurrence" covered by this insurance including but not limited to, loss resulting from:

a. Your inability to realize income that you would have realized had there been no loss of, or loss from damage to, Covered Property...

b. Payment of costs, fees or other expenses you incur in establishing either the existence or the amount of loss under this insurance.

The same issues arise for claims based on lost profit calculations. If an insured projected a profit of $500,000 but achieved a profit of only $200,000, the insured may attribute the $300,000 difference to the dishonest employee.

Although an insured can use an inventory or profit computation to help support a claimed loss amount, this method, generally, will not provide sufficient proof for a claim. Unless the insured can demonstrate, in an irrefutable way, that the only explanation for the shortage could be through the act of an employee, any claim presented will likely fail.

Figure 3-4. Standard Inventory Loss Exclusion

INVENTORY SHORTAGES EXCLUSION

Loss, or that part of any loss, the proof of which as to its existence or amount is dependent upon (1) an inventory computation; or (2) a profit or loss computation.

Source: Employee Dishonesty Coverage Form (CR 00 01)

Therefore an insured should meticulously outline the method the employee used to perpetrate the theft to demonstrate that the employee had the necessary access to perform the dishonest act, and should also present all documents that connect the employee to the claimed loss. For example, if part of the dishonesty involved the alteration of shipping receipts, the insured should provide all the altered receipts to the insurer. Although these documents may not directly support the loss amount, they will connect the employee to the dishonesty and support the method by which the dishonesty occurred.

Is this documentation enough to assure a full recovery? Maybe not; however, every link between the employee and the claimed loss strengthens the insured's claim.

Figure 3-5. Loan Loss Exclusion

LOAN LOSS EXCLUSION

This bond does not cover... (e) loss resulting directly or indirectly from the complete or partial nonpayment of, or default upon, any Loan or transaction involving the Insured as lender or borrower, or extension of credit, including the purchase, discounting or other acquisition of false or genuine accounts, invoices, notes, agreements or Evidence of Debt, whether such Loan, transaction, or extension was procured in good faith or through trick, artifice, fraud or false pretense, except when covered under Insuring Agreement A [Employee Dishonesty], (d) or (E)...

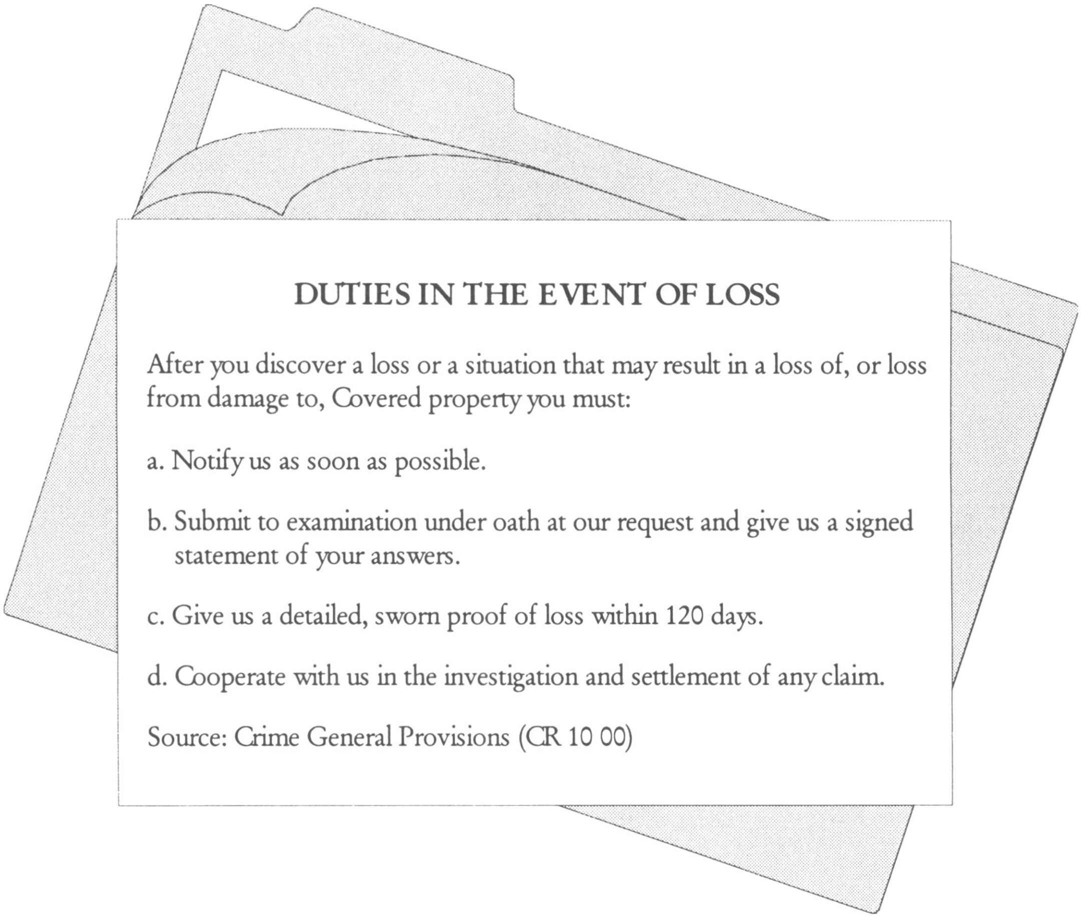
Loan Loss

This chapter has focused on the standard provisions of a Commercial Crime Policy. Although not part of a Commercial Crime Policy, the loan loss exclusion is worthy of special mention. See figure 3-5 for an example of a loan loss exclusion taken from a Financial Institution Bond.

This language establishes that the bond does not cover all risks; specifically, it avoids coverage for credit decisions. The bond's language seems clear, particularly because the wording even stipulates that loans obtained through "trick, artifice, [or] fraud" are excluded.

You can obtain coverage for loan losses generated by a dishonest employee who had the manifest intent both to cause a loss and to obtain a financial benefit. In addition, the insurer may specify in the bond that it will cover those loan losses when an employee was in collusion with one or more parties to the transaction and the employee received, as a result of the dishonesty, a financial benefit with a value of at least $2,500.

Figure 3-6. Insured's Duties to Insurer in the Event of Loss



DUTIES IN THE EVENT OF LOSS

After you discover a loss or a situation that may result in a loss of, or loss from damage to, Covered property you must:

a. Notify us as soon as possible.

b. Submit to examination under oath at our request and give us a signed statement of your answers.

c. Give us a detailed, sworn proof of loss within 120 days.

d. Cooperate with us in the investigation and settlement of any claim.

Source: Crime General Provisions (CR 10 00)

3.4 Insured's Responsibilities in the Event of a Loss

3.4.1 Duties of the Insured

Dishonesty policies typically impose several duties that the insured must fulfill in order to protect its ability to recover under the terms of the policy once a loss is discovered. In all cases, the insured should take action to prevent further loss and take the appropriate steps to mitigate the damage and recover from any loss sustained. These duties include:

- Giving timely notice of potential loss
- Filing a proof-of-loss form
- Cooperating with any insurance investigation

See figure 3-6 for an example of the specific language used in a Commercial Crime Policy to spell out the insured's duties.

Most dishonesty policies typically contain two additional obligations for the insured. The obligations are (1) agreeing not to prejudice the rights of the insurance carrier and (2) accepting the procedures for filing a law suit in the event of a claim denial. See section 3.4.2 for more information on these duties.

3.4.2 Handling the Discovery of Employee Dishonesty

It's a call that all executives dread—internal audit reveals that the controller has been diverting corporate funds for his or her personal use. The discovery spawns a myriad of questions and problems, all of which require quick solutions.

Dealing with an allegation of wrongdoing against an employee is never easy. Invariably it provokes feelings of shock and betrayal within the firm, and often causes a decline in internal morale and external goodwill. It may also hurt the bottom line, depending on the extent of the loss and, most critically, whether the loss is covered by fidelity insurance.

You must deal with dishonest acts, whether you report to the police and pursue aggressively or handle discreetly within the organization. In either case, the actions you take will have a critical bearing on whether or not you can recover under your fidelity insurance. Therefore, it is important to know how to respond when allegations of wrongdoing arise. Most victims (and even most claims adjusters), however, rarely deal with these types of situations, and, as a result, these claims are often learning experiences for all concerned.

Victims of dishonesty should never forget that it is their property that has been lost. There can be no relaxed attitude when responding to this kind of incident. You must conduct yourself as if no insurance existed, including making efforts to minimize or prevent further loss and initiating procedings for maximum recovery.

On the issue of recovery, it is important to note the *right of first recovery* provisions in fidelity coverage. Typically, where a loss does not exceed the policy limit and recoveries are made, the *right of first recovery* is to the underwriter and then to the insured, to satisfy any policy deductible. However, if the loss exceeds the policy coverage amount, the right of first recovery is to the insured for the amount of the loss in excess of the bond coverage only, and then the aforementioned rule applies.

3.4.3 A Course of Action

The first decision to make on the discovery of any form of dishonesty is whether or not to conduct an investigation. Some victims choose not to proceed even when they have fidelity coverage. They consider the potential cost of an investigation, including the time lost internally, combined with external investigators' costs and legal fees, among other costs, to be prohibitive.

There are many reasons to proceed with an investigation. The loss may be covered under the fidelity insurance and therefore would be recoverable. In addition, there may be more to the dishonest scheme than was initially manifest. Failing to investigate and take appropriate action when the crime is first discovered may prejudice the insurer's rights and result in coverage denial when the true extent of the loss surfaces. Similarly, there may be more people involved than originally believed, which could make any initial corrective actions ineffective.

A victim that fails to report a loss or reports a loss late risks the possibility of a subsequent coverage denial. The typical policy includes the standard requirement for reporting a loss as soon as possible (see section 3.4.4). In addition, the insurer also immediately cancels coverage for any employee discovered by the insured (or the insured's partners, officers, or directors) to have committed any dishonest act. Therefore, it is extremely risky to continue the employment of an individual who has defrauded or stolen from the company. If management determines that the best course is to continue the employment of the dishonest employee, management should consult with the insurer and request a waiver of the provision canceling coverage for that employee.

Assuming the organization decides to proceed with an investigation, management should assign a representative of the firm the responsibility of coordinating the organization's efforts to investigate, document, and prepare a proof of loss. In view of the timing obligations under the policy, this individual should immediately be available to devote considerable time to the claim. This *claim coordinator* should have a financial background and the authority to cross departmental boundaries because the loss investigation will undoubtedly involve numerous departments. The claim coordinator also must thoroughly understand the policy before an in-depth investigation can begin. The claim coordinator, along with legal counsel, should bear responsibility for all communications with the dishonest employee, the insurer, and its representatives, including the insurance agent.

3.4.4 Notice of Loss

As discussed previously, immediate action after discovery is critical because discovery triggers the policy's notice and proof-of loss timing requirements. The policy requires the insured to notify the insurer as soon as possible after a potential covered-loss situation is discovered. Notice can be provided by telephone; however, best practice is to send a written follow-up notification. Although the coverage states "as soon as possible," sooner is always better than later, as the date of notification is determined by the circumstances of the case and can become a question for a jury. One jury found seventeen days to be an unreasonable delay in notifying the insurer, but in another case, a fifteen-month delay was not deemed unreasonable.

Some victims opt to allow the dishonest individual to continue his or her wrongdoing in an attempt to gather evidence. This is not advisable because, as previously discussed, an insurer will cancel coverage for any dishonest employee immediately upon discovery, and, therefore, the policy will not cover subsequent losses.

When providing notice, it is not necessary to develop all the facts or even the extent of the loss. After a more comprehensive investigation, the insured can then provide the details of the claim in the form of a written, and sworn to, proof of loss. The policy typically requires that the insured file the proof of loss within 120 days from the time it discovers the covered act—not from the time the insured gave notice. If it is not possible to comply with the 120-day deadline, ask for an extension—in advance—from the insurer, requesting a response in writing. Most insurers will accommodate this request, thereby providing an extension under a reservation of rights.

3.4.5 Supporting Documents

Although insurers value statements made by the dishonest employee, they also require documentation supporting the claim of dishonesty and the resulting loss amount. Make it a priority to obtain and secure the relevant documents. Verify what may seem obvious or conclusive in appearance using the most complete documentation possible. Use discussions with other employees to determine the existence and importance of the documentation.

Early in the investigation, identify those employees who may be able to assist in the loss calculation. While there are a myriad of factors that affect the timing and appropriateness of interviewing these employees, remember that over time memories not only fade but become selective. Conduct these interviews individually, and take detailed notes. Whenever possible, the claim coordinator should attend all interviews.

3.5 The Insurer

3.5.1 The Insurer's Investigation

After receiving the proof of loss, the insurer may send in an independent investigator to analyze the claim. Start preparing for this investigation by designating one contact person—usually the claim coordinator. This designated contact should act as liaison for all requests from and discussions with the insurer's representative.

3.5.2 Subrogation Rights and Duties

If the insurer pays any portion of the claim, the insurer is subrogated to the insured's recovery rights. This is covered under Section B 17 of the *crime general conditions* policy form.

Although subrogation is thought of as arising in the context of a resolved claim, subrogation also imposes a further duty on the insured long before resolution. The insured must, in no way, jeopardize the subrogation rights of the insurer.

However, if the insured has the opportunity to maximize its recovery as a result of accepting a settlement offer from the dishonest employee or the employee's attorney, the insured could appear to be acting contrary to the language of the subrogation provision. In this case, the insured should bring the settlement offer to the attention of the insurer and demonstrate its benefits. Generally speaking, insurers will agree to reasonable settlement offers. As always, get all such "side agreements" with the insurer in writing.

3.5.3 Response to a Claim Denial

The game is not necessarily over when an insurer denies a claim. Request a detailed, written explanation for the denial. Ask independent advisers to carefully review the claim and the rationale for the coverage denial to determine whether the denial is warranted. If you can make a good argument for coverage and it becomes necessary to file a lawsuit against the insurer to invoke coverage, the provision form stipulates certain procedures for the insured to follow (see figure 3-7.)

Figure 3-7. Legal Action Against Insurer Provision

LEGAL ACTION AGAINST INSURER PROVISION

You may not bring any legal action against us involving loss:

a. Unless you have complied with all of the terms of this insurance;

b. Until 90 days after you have filed proof of loss with us; and

c. Unless brought within 2 years from the date you discover the loss.

Source: Crime General Provisions (CR 10 00)

As stated in the clause in figure 3-7, the insured must give the insurer at least 90 days from the day the proof of loss was filed, so that the insurer may investigate and make a decision about the claim, before the insured may file a lawsuit against the insurer. However, the insured also is limited in the amount of time permitted to bring such an action: within two years after discovery of the crime.

3.5.4 Summary

Fortunately, most organizations experience few employee dishonesty losses of any consequence. The strict policy requirements and sensitive nature of the investigation required to document claims and the entire process of asserting a fidelity coverage claim can be quite intimidating. If dealt with in a well thought-out and logical manner, however, you can effectively handle employee dishonesty claims. The process reviewed in this

Handbook should give risk- and insurance-professionals some guidance for planning a response.

3.6 Risk Financing Checklist

See table 3.1 for a checklist designed to assist CPAs to address risk financing and fidelity insurance issues in their organizations and in those of their clients. If necessary, investigate and follow up *No* answers and then document the results. Use the *Ref* column is to cross-reference the checklist to any additional documentation.

The checklist is intended for general guidance and information only. If risk financing is a concern, seek the advice of a risk management specialist.

Table 3.1 Risk Financing Checklist

Risk Financing Checklist	Yes	No	NA	Ref
1. Purchase of Fidelity Insurance Coverage				
a. Has management reviewed operations to determine the nature and extent of potential losses from fraud and commercial crime?	☐	☐	☐	___
b. Has management considered the extent to which the organization can self-finance this risk (that is, could it survive a catastrophic loss without insurance)?	☐	☐	☐	___
c. Has management taken all reasonable steps to remedy any previously identified vulnerable areas of the business or any weaknesses in internal controls?	☐	☐	☐	___
d. Has management established contact with a reputable insurance broker capable of placing the required fidelity coverage?	☐	☐	☐	___
e. Has management assigned an appropriate person the task of liaising with the broker to determine alternative kinds, levels, and costs of coverage, and to report back to management on these alternatives with appropriate recommendations?	☐	☐	☐	___
f. Are procedures in place to provide for the timely and appropriate response to circumstances where dishonesty is identified, suspected or alleged?	☐	☐	☐	___
g. Prior to finalizing the recommended fidelity coverage, has management and, if necessary, legal counsel, carefully reviewed the wording of the policy to ensure the following:	☐	☐	☐	___
• Definitions, exclusions, and other clauses are acceptable and consistent with the nature of the business	☐	☐	☐	___
• When possible, duplication with other insurance (for example, fire and theft policies) has been avoided	☐	☐	☐	___

(continued)

TABLE 3.1 *(continued)*

Risk Financing Checklist	Yes	No	NA	Ref
h. Prior to signing, has management verified all answers to the questions on the application for coverage (for example, where an internal control is indicated, does it exist and is it operating effectively)?	☐	☐	☐	___
i. Prior to signing, has management reviewed the wording of the policy to determine what changes, if any, are required and which of these changes should be made in the conduct of the business, including the following:				
• Hiring-screening of new employees	☐	☐	☐	___
• Use of contract employees, who may not be covered	☐	☐	☐	___
• Bookkeeping and reporting practices	☐	☐	☐	___
• Internal controls	☐	☐	☐	___
2. Maintenance of Fidelity Insurance Coverage				
a. Is a mechanism in place to ensure that the organization meets the important terms in the policy in order to keep the policy in good standing, including the following:				
• Paying premiums when due	☐	☐	☐	___
• Reporting any loss incidents to the underwriter, even those below the deductible when no loss claim is filed	☐	☐	☐	___
• Maintaining adequate internal controls and good security practices (for example, locking safes)	☐	☐	☐	___
• Reporting changes in the accounting system	☐	☐	☐	___
• Reporting changes in the nature and scope of operations that may affect risk	☐	☐	☐	___
b. Does the organization review its fidelity coverage on at least an annual basis to ensure that the coverage remains adequate and continues to meet acceptable cost-benefit criteria?	☐	☐	☐	___
c. Does the organization assess its risk and its financing through fidelity insurance on at least an annual basis?	☐	☐	☐	___
3. Discovery of Dishonesty and Fidelity Insurance Claims				
a. Immediately upon suspicion or discovery of a loss incident, has the organization implemented the following steps:				
• Protection of assets from further loss	☐	☐	☐	___
• Preservation relevant documentation and other evidence	☐	☐	☐	___
• Notification of the underwriter by hand delivery or registered (certified) mail ("return receipt requested")	☐	☐	☐	___
• Involvement of legal counsel and a claim coordinator	☐	☐	☐	___

TABLE 3.1 *(continued)*

Risk Financing Checklist	Yes	No	NA	Ref
Never ignore this issue; you must act as if there is no insurance				
b. Internally, or in cooperation with the underwriter (or both), are adequate resources in place to undertake a thorough and timely investigation?	☐	☐	☐	___
c. After establishing reasonable suspicion of a criminal act, has management called in the police?	☐	☐	☐	___
d. Has management ensured that no actions are taken to prejudice the insurance claim, or the underwriter's ability to make recoveries, or both (for example, obtain underwriter's permission before reaching settlement with third parties or suspected perpetrators)?	☐	☐	☐	___
e. Has management considered initiating legal proceedings to ensure maximum recovery?	☐	☐	☐	___
f. Are adequate personnel and procedures in place to perform the following:	☐	☐	☐	___
• Document the insurance claim (that is, the Proof of Loss)	☐	☐	☐	___
• Follow up with the underwriter as required until the claim is settled	☐	☐	☐	___

Computer Security
and System Recovery

CHAPTER 4:

Computer Security and System Recovery

CHAPTER 4:

Computer Security and System Recovery

4.1 The Role of Computers in Modern Corporations

It is impossible to overstate the importance of computers in the modern corporation. Computers track all assets, manage accounting, handle word processing, operate phone and voicemail systems, and control communications. Computers have evolved from large mainframes to networks of PCs—each of which has capabilities greater than those mainframes from the sixties and seventies—to provide a wide range of services to the modern corporation.

If those computers fail or are compromised, whether by accident or by deliberate action, the company is in trouble. Preventing an incident is infinitely preferable to dealing with one. If an incident occurs, however, the corporation must have a way of recovering operations quickly and efficiently. Therefore, the establishment of appropriate computer security and system recovery is a vital function of any organization.

Make no mistake—computer security is a complex subject that is growing and becoming more complex every day. Businesses spend many billions of dollars each year on hardware and software to control access to computers, to secure the data they contain, and to detect intrusions. They invest hundreds of millions more in systems that permit efficient recovery should a problem occur. There are firms, some with thousands of employees, specializing in computer security. Clearly, this is a highly specialized field. One chapter in a Handbook cannot make you an expert in computer security, and it is not intended to do so.

This chapter orients you to the field of computer security so that you, as a CPA, can be certain not only to handle computer security and systems recovery appropriately, but also to consider the major risk factors.

4.2 Management's Security Issues

In the modern, global business environment, the computer has evolved from being a *number cruncher* used by the accounting department and tended by a priesthood of mathematical geniuses in a glass-fronted fire-protected computer room, to infiltrate virtually every facet of the corporation. The computer has replaced typewriters with word processors, adding machines with spreadsheets, and voluminous physical files with database programs. In many companies, all significant information concerning assets, transactions and operations are held on one or more computers. Today's organization likely makes use of hundreds of computers connected in local area networks (LANs) and wide area networks (WANs). An organization may have dozens of these networks, each using servers ranging from PCs to mainframes.

4.2.1 Components of Security

Data Communications

Businesses do not exist in a vacuum. Increasingly companies are dedicating more resources to data communications. Many companies—perhaps most, by now—have moved onto the Internet, both as a way of distributing information (usually on the World Wide Web) and of transmitting information between people or units: this includes electronic mail (email) and the use of File Transfer Protocol (FTP) to move files across the Internet. The space on business cards that formerly held a Telex address now has an email address.

Some companies are developing and fielding what are sometimes called *extranets,* which link their suppliers and distributors through Internet connections. Other businesses, seeking more security than is provided on the global public Internet, have turned to private network providers who operate worldwide data communications networks that use the same tools and protocols as the Internet, but are limited in use to subscribers.

Security and System Structure

Before computers, businesses achieved information security by installing locks on file cabinets and file-room doors, and by restricting access to various files and documents. During the initial period of centralization, organizations used mainframe computers with attached terminals; effective access control existed on the central system. Today, the situation is different. How is it possible to secure computer networks and data communications structures that are not only complex, but also may exist on a global scale?

As businesses increasingly rely on computers and networks, they have an increased need to secure their information-processing infrastructure against accidental or deliberate damage and to provide an efficient, effective and secure system for backup of data and programs on a regular basis. Organizations need security systems to restore information following an incident or outage. Systems are virtually impossible to manage and keep secure if they are not properly organized and structured. As a key aspect of security and recovery, and as a measure of preventative maintenance, businesses should implement a structure for organizing and storing information (for example, data files, spreadsheets, word processing documents, and so on). In developing an effective information storage structure, you should consider issues, such as file nomenclature and file access privileges.

External Versus Internal Security

As people recognize information to have enormous value, sometimes a value greater than anything else in the organization, their need to safeguard this information has increased. However, the risks inherent in the processing, storage and transmission of that data have also increased, particularly as the Internet has flourished. There have been many documented cases of industrial and economic espionage designed by organizations attempting to jump-start their business activities by stealing proprietary information.

Companies have also been victimized because management believed the major risk they faced was from outside the organization. They spent substantial resources on firewalls and very little on other forms of security. Unfortunately, every study indicates that where crime against business is concerned, 80 percent or more of that crime is perpetuated within the company and hence, from inside the firewall.

As systems grow more complex, with increasingly greater speed in connecting to the Internet, it is important when assessing security that you consider a wide range of threats and a wide range of ways in which to thwart those threats. Although an outsider can hack into your network to gain access to a specific file, an insider might be able to pick up a carelessly stored backup tape and walk out with a copy of every file in your system, all recorded on a tape so small that it can be secreted in a shirt pocket.

Therefore no one should question the need for computer security and the ability to recover from problems both natural and human-generated. However, it is useful to focus on some of management's key concerns.

4.2.2 Management's Key Concerns

Managers in business and government have recognized the growing importance of computer processing to their organizations and, over the last few years, have expressed their concerns in a wide variety of publications. These concerns generally fall into one of the following three categories.

1. Theft of confidential information
2. Information integrity
3. System availability

Each of these concerns is addressed below.

Theft of Confidential Information

Recognizing that companies increasingly store more information in computer systems, management must have assurance that this information is well protected and that only appropriately authorized employees have access.

For example, theft of proposed pay scales prior to labor negotiations could be detrimental to the process and result in increased production costs. Theft of marketing or pricing plans might result in a loss of competitive advantage. Similarly, theft of personal or financial customer information could result not only in embarrassment, but also in a direct loss of business and possible litigation. The threat of the loss of valuable intellectual property has become so great that the government has enacted the Electronic Espionage Act, making the theft of intellectual property a federal crime, punishable with up to ten years imprisonment.

Information Integrity

Because of the large volume of information processed by computers, it is not usually feasible to confirm the validity or accuracy of processing results. Therefore, management seeks assurance on the integrity of computer-generated information: that the information is reasonably protected against unauthorized tampering by employees, computer viruses, hackers, or other forms of sabotage.

For example, tampering that results in inaccurate reporting of sales figures could, in turn, cause inappropriate production, excessive inventory levels, and lost product sales.

Unauthorized altering of the accounts-payable records could result in incorrect mailing labels or inaccurate shipping amounts, and therefore, direct financial loss.

System Availability

Recognizing their organization's dependence on the data processing service, management needs to be reassured, not only that everything has been done to reduce the likelihood of disruption, but also that there are plans in place for resuming data processing in the unlikely event of a major catastrophe. The total or partial loss of data processing services would make it difficult, if not impossible, for most organizations to perform routine business operations.

4.2.3 Effective Computer Security Systems

An effective computer security program can help to manage and, to an extent, alleviate the above concerns. The design of an effective computer security program must take into account the nature of the risk, and the nature and cost of the controls required to reduce exposure. Note that there is no such thing as 100 percent protection. The growth of networking and particularly of the Internet has materially increased the risk of computer crimes and incidents. The following areas are among those that management must address.

Accidental Versus Deliberate Events

The events that result in breaches in confidentiality, integrity or availability may be accidental or deliberate in nature, and may be the result of actions either internal or external to an organization.

On a day-to-day basis, management could trace most incidents to internal accidents, such as an employee entering incorrect data or inadvertently deleting an essential file. Accidents also include failures arising out of undiscovered program errors, or bugs.

Some systems are composed of software packages procured from manufacturers. Others are completely custom written. Others—perhaps most these days—are a combination of procured software and custom code. In any case, the systems that support an organization may consist of tens or even hundreds of thousands of lines of code. It is virtually impossible to test every possible condition that might occur in these immensely complex systems. Program bugs exist in every major system. With the marketplace demanding speedier program development cycles, manufacturers have converted at least a part of their traditional testing procedures into *beta testing*, in which the manufacturers release an advance version of the software to customers to assess its capabilities.

It is important to understand the difference between beta testing and the more traditional system testing. In system testing, the software is stressed with deliberate input errors, processing problems and anything else the testing team can do to cause the software to fail. In beta testing, the users are not deliberately stressing the system in an attempt to make it break down. Nonetheless, commercial-software beta testing is valuable, and results in reports to the manufacturer of hundreds, or even thousands, of potential program bugs. Regardless of how thoroughly a program is tested, it can still fail, and fail disastrously, as the result of an accidental bug.

Prevention, Detection and Recovery Controls

Prevention is the best and most effective way to minimize the impact of an unwanted event that could affect information confidentiality, integrity or availability. In the case of deliberate acts, preventive controls will reduce opportunity and thereby remove temptation. Another important factor in preventive control is the notion of deterrence, which forms a belief in the mind of would-be perpetrators that they are likely to be caught if they attempt a computer-related crime.

Preventive controls, however, cannot provide a 100 percent guarantee that a problem will not occur. As a result, organizations typically use complementary detective controls to highlight any actual or attempted security violation. For example, existing software features may prevent unauthorized users from gaining access to data. In these situations, the software is programmed to produce reports that document all attempts by unauthorized users—a feature known as detective control.

In addition to preventive and detective controls, organizations must prepare in advance for recovery from unexpected events. For example, the backup-copy feature used to retrieve a deleted data file constitutes a recovery control.

A well-designed security program includes elements of all three types of control:

1. Preventive
2. Detective
3. Recovery

The mix of controls used depends on the nature of the information stored on the computer, combined with the reliance placed on the computer, and management's willingness to accept the associated risks. In the rapidly changing global environment in which we work, with Internet connectivity growing at an unprecedented rate, and new equipment and software becoming obsolete in months, it is no simple matter to keep security features up to date with potential threats.

4.3 PHYSICAL SECURITY

Physical security is the generic term used to describe the protection of the computing facility. The controls exercised under the heading physical security are typically preventive and detective in nature.

Many may think that physical security has become unimportant in the age of the personal computer, when virtually every employee has a powerful workstation with a fast processor and access to company networks, which are often equipped with huge local storage disk drives. But the reality is that mid- to large-size organizations still use midrange computers (such as the IBM AS400, Digital Vax and Alpha systems, HP 9000s, and similar systems from other manufacturers) and mainframes (such as the IBM System 390 and large scale DEC, SUN, HP, and Unisys machines). Even managers at companies that base their computing on a LAN often realize that they best protect their servers by placing them in a dedicated and protected operating facility.

Physical security primarily addresses the accessibility concern, and attempts to minimize the potential for system loss as a result of equipment damage. To achieve physical security, consider each of the following areas:

1. Computer Room Construction
2. Fire Detection and Suppression
3. Water Protection
4. Electrical Power Reliability
5. Environmental Control
6. Physical Access Controls
7. Physical Security for PCs

Details on each of the components of physical security follow.

4.3.1 Computer Room Construction

The National Fire Prevention Association (NFPA) standards provide the most concise specifications for recommended mainframe, midrange and server computer room construction. In summary, to provide an appropriate level of protection, computer room perimeter walls should be constructed to a minimum of a one-hour fire resistance rating. These walls should extend from concrete ceiling to concrete floor (slab to slab). Obviously, slab-to-slab walls also serve to protect the facility against unauthorized entry from over a false ceiling or under a raised floor.

This construction minimizes the possibility of fires originating in general office areas migrating to the computer room before they can be extinguished. The use of glass partitions to segregate the computer room from the general office environment usually does not provide sufficient protection against a migrating fire.

Computer rooms have come full circle. During the sixties and seventies, the only computers in most organizations were large mainframes kept in presumably secure computer rooms. As companies changed from central computers to client-server environments, file servers, which had become the departmental version of a mainframe, did not need special environments. They were placed anywhere—on the floor, under a table, or sometimes in a closet. This led to a lot of problems. Often they were accidentally turned off or damaged. They did not always have power protection, and on more than one occasion, companies suffered when someone accidentally pulled the server's plug from the wall. With servers in a closet or under someone's desk, backup was sometimes forgotten, and even when carried out, the backup tapes were often stored adjacent to the server.

4.3.2 Fire Detection and Suppression

Fire detection and suppression systems are essential in the computer room to protect the investment in computer equipment and the information stored thereon. These systems are designed to detect and suppress fire before it advances to a serious state. Security experts recommend automated detection and suppression systems because these systems reduce the dependence on manual fire- fighting techniques that may prove either unsatisfactory or late in arrival.

The most common fire suppression systems are water sprinklers and various fire-suppressing gasses. A gas, Halon 1301, formerly the most popular fire suppression gas, is no longer manufactured because it turned out to be a significant environmental hazard.

Water sprinkler systems may be "wet" or "dry." Wet systems contain water in the pipes at all times. Dry pipe systems, also called *pre-action* systems, do not contain water until an alarm situation occurs (usually involving a products-of-combustion detection unit), at which point a valve automatically opens to charge the system. A high-temperature event must also occur to open a sprinkler head.

Fire detection systems can also provide a direct linkage to other significant support functions, such as opening fire exits, shutting off equipment and fans, and providing immediate notification to an alarm company or the fire department via a communications link.

4.3.3 Water Protection

Water and electrical systems do not mix, but both are generally found in computer rooms protected by sprinkler systems. Water can also enter computer rooms through leaks that may originate on another floor of the building. Therefore, it is vitally important to ensure that precautions are taken to detect and remove water leakage before it contacts the electrical supply. Water protection usually involves the provision of:

- Underfloor water detectors, normally in the vicinity of air-conditioning units. Water detection systems are usually monitored in the same manner as fire alarms.
- Floor drains to remove any water buildup. Unless specified during construction, floor drains typically are not provided in modern office towers.
- Waterproof equipment covers. Where sprinkler systems or other above-floor water sources are present, you should have available equipment covers or rolls of plastic that can be pulled over the equipment in the event of a problem.

4.3.4 Electrical Power Reliability

Unless suitable precautions are taken, a disruption to the electrical power supply will result in the loss of computer service. The provision of backup power sources can be expensive, and it may not be cost justified if the computer center is located in an area where the electric power supply is reliable. If the electric power supply is unreliable, or the nature of processing critical, consider using uninterruptible power supply (UPS) and backup generators.

Uninterruptible Power Supply (UPS)

UPS provides battery backup in the event of power failures or brownouts. The regular power supply is monitored at all times, and battery power automatically provided when required. These systems have become increasingly affordable.

Backup Generators

Backup generators are recommended because UPS can only provide battery backup power for a limited time. In computer centers that provide critical processing services or in areas where electric power is unreliable, diesel generators that can produce electric power for an indefinite period, provided fuel is available, often support UPS systems. Finally, regardless of the local power supply outage record, it is likely that power conditioners will be used in larger computer installations, and surge suppressors will be provided for desktop PCs. Power conditioners and surge protectors monitor the electric power supply and remove voltage sags and surges.

4.3.5 Environmental Control

Environmental control is an issue that primarily has been a concern for larger mainframe computer environments. Even the users of the smaller machines, whose manufacturers claim can operate in a general office environment, cannot totally ignore the following environmental issues:

1. Temperature
2. Humidity control
3. Environmental contamination

Temperature Control

Computers cannot operate in extreme temperatures. It is true that the range of operating temperatures has increased over the years. However, even when the specifications indicate that the machine will operate in a wide temperature range (for example, 59–90 degrees Fahrenheit or 15–32 degrees Celsius), it is not advisable to operate these machines near either the lower or upper limits. Air conditioning is usually installed to reduce the likelihood of system outage or damage as a result of overheating.

Humidity Control

The computer manufacturers normally indicate a range of humidity that is acceptable for their machines, for example a 20–80 percent humidity tolerance. Normally the air conditioning unit provides humidity control.

Environmental Contamination

Dust can cause major problems in a computer environment. If dust gets into a disk pack, it may cause a head crash, making information on that disk inaccessible. In addition, accumulations of paper dust from printers are a potential fire hazard. To minimize the potential for dust contamination, you should regularly vacuum the areas where dust normally accumulates.

4.3.6 Physical Access Controls

The importance of physical access controls over all assets and related records is obvious. Such controls help to reduce the risk of fraud and commercial crime because—

- Physical access controls are often the most visible to potential perpetrators. Strong controls in this area send a powerful deterrent message vis-à-vis the other controls in the system. Conversely, loose physical controls invite challenge.
- Perpetrators of many frauds must come into physical contact with either the asset being misappropriated or the related asset records in order to cover up the fraud. Reducing physical access reduces opportunity.

- Access controls that fail to prevent fraud and commercial crime still often assist in the investigation process, for example, the determination of what actually happened and the narrowing of the list of possible suspects.

Physical security over computer installations and equipment is particularly important. Sometimes white-collar criminals and irate employees can resort to blue-collar crimes, such as arson and the willful destruction of property. When this happens, these blue-collar crimes may be classified as commercial or economic in nature.

The only employees who should require access to computer equipment are those responsible for its operation. Any third party engineers performing maintenance should be accompanied by operations staff at all times. Providing more access increases the potential for vandalism, mischief and human error; any of these threats could result in processing disruptions.

Limiting access to the computer room involves securing the doors and keeping them closed at all times. There are a variety of devices available for achieving this, the most common include—

- *Key locks:* These are the cheapest to install but are usually the least secure because duplicate keys can be made and distributed without control.
- *Cipher locks:* These are push button combination devices and are generally more secure, provided the combination is changed on a regular basis.
- *Card access devices:* These are probably the most secure mechanisms because cards cannot be readily duplicated and card distribution can be controlled.

4.3.7 Physical Security for PCs

Much of the preceding discussion relates to computer systems of any size. Some especially important measures necessary to physically secure PCs follow:

- Restrict physical access. Lock doors during off hours or when an office is vacant, or both.
- Use the security features provided on many PCs, such as passwords, which prevent access by unauthorized individuals.
- Ensure that all employees watch for unauthorized personnel in areas where microcomputers are located.

4.4 Logical Security

Logical security is the term used to describe the protection of information stored on a computer system. The controls involved are usually a blend of preventive and detective controls. Organizations use logical security to address confidentiality and integrity concerns, and to reduce the potential for inappropriate information disclosure, modification or deletion.

Achieving an appropriate level of logical security involves giving thought to how the user gains access to information. In addition to the security controls for the data itself, you should consider the controls over the software that provide access to the data and to the system. In so doing, keep in mind the following:

- Communications security
- Data security
- Software integrity
- Computer operations security
- Logical security for microcomputers

A description of each follows.

4.4.1 Communications Security

Communications security focuses on controlling the various methods of access to the computer system. Of course, communications security primarily serves to ensure that valid transmissions between computer systems are complete and accurate. As an added benefit, communications security also presents an obstacle to criminal activity.

Passwords and Administration

A valid user identification (ID) and password is the first line of access control on most computer systems. The validation of the ID and password by a computer program represents the preventive part of the control while the rejection and recording of an invalid ID or password represents the detection control. To be effective, the detective aspect of password control requires an investigation of all reported access failures.

For effective password controls, procedures should be installed to ensure that—

1. Users choose passwords that are not simplistic in nature; for example, because simplistic passwords can be readily guessed and the system compromised, never use initials, a spouse's name, or other similar personal passwords.
2. Management distributes new user IDs and passwords to users in a controlled manner.
3. Users change passwords regularly, approximately every 30–90 days, depending on the nature of the information accessed.
4. Management revokes IDs and passwords of users who have left the organization. Similarly, when users move from job to job within an organization, management modifies their access rights so they can only access the data required for their current job.

Network Security Features

The programmed network security features that are available vary from system to system. Some of the common features include—

- A maximum number of log-on attempts. If the user has not successfully logged on in the specified number of attempts, the session is terminated and the incident is recorded on a log for investigation. On some systems, the user's account is locked to prohibit further attempts until the operators or the security-officer function takes action. This feature is designed to prevent unauthorized users from repeatedly attempting to gain access.
- Automatic log-off of inactive terminals. If an employee leaves a terminal logged-on, anyone who gains access to that terminal has the access rights of the previous user, thereby breaching password security. Therefore, many systems automatically log off users when the terminal has been inactive for a defined period of time.

- Restrictions of users to specific terminals, specific times of the day, or both.
- Echo checking of transmitted information to ensure the information is complete and accurate. This is achieved by a retransmission of the message to the source terminal for validation.
- Firewalls to provide the security necessary to control unauthorized access to the system from the Internet. Ranging from relatively simple hardware or software to complex and hard-to-maintain packages, firewalls have become a requirement for systems attached to the Internet. Careful installation is essential to prevent making unintended access points available to an invader.

Remote-Access Security

Hackers have received considerable publicity in recent years, after successfully gaining access to numerous computer systems. In response to the problems created by hackers, several companies have developed and marketed security devices to limit remote access to authorized employees.

One common device available to help control dial-up computer access is the callback device. When an employee dials in, the callback device intercepts the call, the employee enters a special code, and the device then *calls back* the phone number associated with the code entered. The communications link is then established and the user ID and password are entered in the normal way.

For both dial-up access and Internet access, there are a number of devices that provide security by effectively providing authorized users with a new password for every log-on. Some systems accomplish this by providing the user with a small key-chain-sized device called a token, which has a window that displays a new code every minute. The user must enter this code along with a memorized password to gain access.

Another version looks much like a calculator. When a user requests access, the system provides a random number (called a challenge) that the user then enters into the *special calculator* with a password. The calculator then displays another number (the response), which is entered into the system to gain access.

Another class of access control, based on biometrics, involves measurement of a physical characteristic. Currently manufacturers offer devices that can check identity based on fingerprints, hand geometry, iris or retinal pattern, or facial geometry. Systems based on voiceprint or signature dynamics are also under development.

4.4.2 Data Security

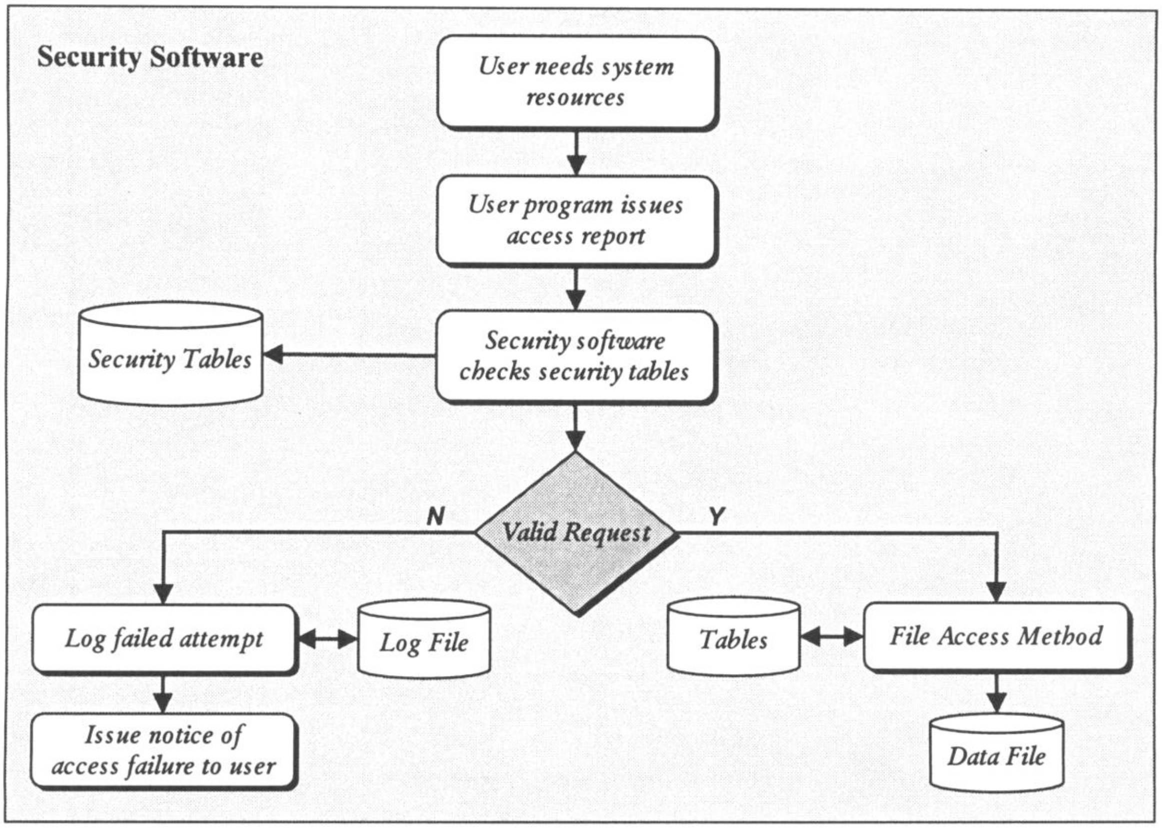
Unauthorized access to information can result in its disclosure, modification or deletion. To achieve efficient data security, you should implement a system capable of evaluating the sensitivity of the data to provide a level of protection commensurate with the nature and perceived value of the information. Data security addresses the issue of protecting information stored on computer files, magnetic media, and hard copy reports.

On-line Data Files

On-line data files are those files stored on disk that users of a computer system can directly access. Two effective techniques are available to secure on-line data files:

1. *Software restrictions.* A program, or series of programs, that references established security tables to determine whether the user is allowed the requested access (for example, read or write) to the requested data file. If the request is valid, the user will be permitted access; if not, access is denied and the access violation is reported on a log file for subsequent investigation. The security software process is illustrated by figure 4-1.

Figure 4-1. The Security Software Process



On some computer systems, the software restriction facility is an integral part of the operating system, while on others a separate security software product that interfaces with the operating system is used.

2. *Data encryption.* This technique scrambles information using a predefined algorithm or key, so that the information is not meaningful to anyone who gains access to the disk file. There are a number of mathematical systems (algorithms) in use as the basis of encryption systems. These systems use keys of various length and complexity. Generally longer keys provide more security than shorter keys. On the Internet all browsers provide some level of security through encryption. Some have short-key capabilities

(generally employing 40-bit keys) that provide a basic level of security, while other versions (often export-restricted) use much stronger 128-bit keys. Some data encryption packages (for example, PGP) can provide for even longer keys (often 1,024 bits in length), which provide incredibly robust security against unauthorized interception. Companies using the Internet to transmit confidential data should seriously consider using encryption to protect that information from unauthorized interception.

Off-line Data Files

Off-line data files are information stored in libraries on magnetic tape, exchangeable disks, and diskettes. Information stored on these media is as readily susceptible to inappropriate disclosure, amendment, and deletion as on-line data files unless it is properly controlled. The preventive controls usually applied include—

- Keeping the media library in a physically secure room where the door is locked whenever authorized staff are not present
- Adhering to media library procedures, which require that the files be issued from the library only for approved purposes, for example, production use and transport to off-site storage

The detective controls normally include an investigation of all materials borrowed, but not returned in a reasonable time, and the performance of periodic inventory checks. However, many smaller organizations consider the use of comprehensive library procedures impractical because of limited staff availability. In these situations and in microcomputer environments, you should regularly back up computer information (on hard disks and diskettes) and store it in a secure location away from the computers.

Reports and Documents

It is easy to become preoccupied with protecting information on computer systems while neglecting information printed on input forms and computer reports. Generally, people rely on internal controls exercised by user departments to ensure that data approved for input is not modified before it is entered into the computer. Frequently, however, people pay less attention to securing input documents before and after input. Yet these input documents contain all of the confidential information ultimately stored on disk.

You should also pay attention to printed output, including—

- *Printing control.* Appropriately destroy any partially printed reports that result from printer problems.
- *Distribution control.* Ensure that the appropriate staff distribute computer-printed reports, particularly reports containing sensitive or confidential information, only to authorized recipients.
- *Storage security.* Staff should secure computer reports in the user department for after office hours protection.
- *Destruction control.* Staff should appropriately destroy all reports when no longer required (this applies to all offices, not just computer areas). Even when information is outdated, improper disclosure may still prove embarrassing.

4.4.3 Software Integrity

The integrity of information depends on the integrity of the programs that produce and use that information. Information's integrity also depends on the integrity of the communications software, transaction processors, file access software, security software, and operating system—known collectively as the system software, which control the operation of, and may be used by, application programs. Software integrity refers to the protection of all system software stored on magnetic media and the migration of programs to production.

On-line Software Libraries

Computer programs are stored on disk files in libraries or software directories. The most effective means of restricting user access to these libraries is through security software restrictions as described earlier in the section, *On-line Data Files*, although library control software may also assist in restricting user access.

The programming staff require access to copies of the programs to perform their job functions. They do not, however, require access to the production versions. Providing programmers with direct access to production versions compromises software control and increases the possibility that unauthorized changes may be made. In general, only qualified *production librarians* should require access to the production programs, and those individuals should copy only new versions of programs into production, as required.

Off-line Software

Off-line software refers to the backup copies of program libraries or directories stored on magnetic tape, exchangeable disks, and diskettes. The controls required to secure these versions of the software are identical to those described earlier in this chapter in the section, "Off-line Data Files."

Migration of Programs to Production

If a programmer can gain access to a program and make changes between the program tests being performed by the user and the program being put into production, the version used in production may not be the same version that was originally tested and approved. Changes may be introduced that could impact information integrity and expose the organization to financial loss. Organizations can address this problem in a variety of ways including—

- Restricting access to the test version of the program to the users who are running the test and the individual(s) who are performing the librarian function responsible for the transfer to production.
- Recording and monitoring the time when the last change was made, provided the system or library control software retains that information. The date of the last change should not be later than the date the tests were run and the software approved for use.

4.4.4 Computer Operations Security

Improper operator intervention also can affect the proper operation of computer programs and, therefore, the integrity of information. In particular, computer operators can create problems by—

- Running the incorrect version of a program against the correct data files. This may introduce errors through the use of untested program code or the possibility of fraud through the use of unauthorized code.
- Running the correct version of the program against incorrect versions of data files. Obviously the results produced by this action would be incorrect and could have serious implications.

To effectively control operator activity, you should consider taking certain measures including—

- Restricting an operator's ability to change the Job Control Language. Job Control Language directs the processing of a program and identifies the program to be run and the data files to be used.
- Using internal tape, disk-label checking, or both, to ensure use of the correct file.
- Providing detailed operating instructions to reduce accidental error.
- Monitoring operator intervention by reviewing the computer activity-console logs and investigating unusual activity.
- Reconciling data file totals from run to run, to ensure use of the correct version of the file.

4.4.5 Logical Security for Microcomputers

Some of the important points to note with respect to logical security for PCs include:

- Be wary of leaving sensitive information on hard disks. Consider using removable disk cartridge devices.
- Use cryptic passwords, and don't leave passwords on or near computer workstations.
- Back up hard disks regularly to microcomputer diskettes or tape.
- Remember when erasing a hard disk that the normal erase procedures of some operating systems leave the file on the disk (that is, it may only remove the file from the directory). Even reformatting a PC hard drive does not make the data unrecoverable. To prevent any possible recovery of sensitive files, use the disk-wiping functions provided by commercial hard-drive utilities programs.

4.5 System Recovery

If properly applied, the preventive and detective controls provided by physical and logical security will minimize the possibility of problems occurring. However, problems do occur—either accidental or deliberate. System recovery procedures are intended to assist in implementing an orderly and controlled return to normal operations, in the event of a problem.

You should consider using recovery controls to address any computer related availability concerns. These controls are necessary in order to address short-term problems as well as more catastrophic long-term events.

4.5.1 Recovery from Operational Failures

Operational failures are those problems that occur during the performance of day-to-day processing. Examples include:

- Incorrect file usage
- Disk files deletion
- Disk files destruction
- Job processing failure
- Computer equipment failure

Overcoming problems of this nature requires an appropriate combination of backup and written recovery procedures.

Data File and Software Backup

To protect against accidental or deliberate destruction, for example, by hackers, it is essential that you and your staff regularly make copies of all data files and software libraries-directories. How often is regularly? This will vary from installation to installation. In determining an appropriate backup cycle, you should consider the following factors:

- The frequency at which file managers update the file, library or directory. This will help managers determine when to make backup files. For example, for system software libraries that are rarely changed it may be more effective to make backup copies only after making changes.
- The number of transactions processed each time the file is updated. This total helps managers determine the amount of effort required to reprocess all transactions entered since the last available backup was taken.
- The amount of processing time available for backup.

In the past, a backup cycle was often determined on an application-by-application basis. Today organizations typically take a weekly copy of all files and libraries, and supplement this with daily *incremental* backups. Incremental backups take copies of only those files and libraries that have been updated during the day.

In many firms, employees frequently work off-line from their server, either away from their office or saving files directly to their local drives. To ensure that all necessary data is properly backed-up at appropriate times, you should establish guidelines that stress the importance of the employees moving their work to the server as soon and as often as possible. This not only provides back-up protection in the advent of a personal computer failure, but also maintains a complete data record on the server for back-up purposes.

To assist in recovery from day-to-day operational failures, keep a backup copy of the data files and software—on-site. In addition, send a copy off-site for use in the event of more catastrophic problems, such as when all on-site material is either unavailable or destroyed. (See section 4.5.2.).

Recovery Procedures

In addition to providing backup copies of the files and libraries, provide the required detailed written instructions for the operators so that they may efficiently and effectively recover any necessary files. These procedures are described in most computer operational manuals, and should address issues such as:

- *Application failure recovery measures.* These measures are normally documented for each application and for each job step within the application. These measures describe how operators can restore processing at an earlier point, and reprocess transactions. In some cases when restoring and reprocessing is not possible, the manual should provide direction for obtaining programming or technical support to resolve the problem.
- *Use of utilities to recover from backup copies.* The involvement of operators in recovery varies from organization to organization. In some installations the operators copy the files and libraries to a predefined recovery area on disk, and it is a user or support group's responsibility to copy them from the recovery area to the production area. Other organizations will recover directly to the production areas.
- *Vendor support for equipment failures or head crashes.* Users should document all equipment failures, including details of the request for vendor assistance and the vendor's response.

4.5.2 Disaster Recovery Plans

Disaster recovery plans are intended to assist with recovery from a catastrophic event. They are not intended to deal with day-to-day operational failures. The term *disaster* is used in the broadest sense—it need not be an act of God. As previously noted, white-collar criminals can also arrange disasters to cover up their crimes.

Definition

A disaster recovery plan is a documented description of the action to take, resources to use, and the procedures to follow before, during, and after a disruption of data processing capability.

Given the business communities current reliance on computers, many executives would probably find the loss of the computer center for a lengthy period of time inconceivable. However, the same executive's organization has probably taken no action on developing a contingency plan. A survey completed several years ago suggested that less than 50 percent of the *Fortune 1000* companies had disaster recovery plans, and for the companies that had, only half of the plans were feasible.

Elements of Effective Disaster Recovery Plans

Before disaster occurs, you should take action to ensure that off-site backup is capable of supporting recovery operations. Keep off-site backup copies of data files and software some distance from the principal site so that access to these vital records will not be inaccessible and, therefore, denied in the event of a disaster affecting the local geographic area.

Consider what happened when a train derailed in Mississauga, Ontario (a Toronto suburb) a number of years ago. In this case, the authorities closed access to a sizable city area for five days because of a dangerous chemical spill. Any organization housing both its data center and off-site storage in that geographical area would have had difficulty implementing its disaster recovery plan.

In addition to keeping off-site backup copies of data files and software, consider keeping off-site the supplies of other materials required for processing. Examples include: check stock files, special invoice forms and forms for laser printers, operations documentation, and a copy of the recovery plan.

Perhaps documenting detailed recovery procedures and implementing regular tests of the recovery plan are the most important actions to take before the advent of a disaster. Disaster recovery operations require the channeling of information to management to assist in decision making during the chaos of a disaster. Without clearly identifying reporting channels and decision points in advance, employees may later take inappropriate action.

Similarly, prepare detailed procedures for system recovery because operations staff may not perform standard procedures as expected when affected by the stress created by a disaster. Remember that in a disaster personnel who might be expected to participate in the recovery—either on the operations team or the management team—may be victims of the disaster, so the plan must make allowances by designating one or more alternates for each recovery position. Regular testing ensures that the plan is workable, and helps to keep the plan current.

During the disaster, the staff with recovery responsibilities should follow documented procedures to—

1. Notify all necessary parties that a problem has occurred.
2. Assess the extent of the damage and the expected period of system outage for communications to the recovery team.
3. Report to a predetermined emergency control center.

After invoking the disaster recovery plan, the recovery staff should follow the documented procedures for—

1. Recovering the critical systems at the identified alternative processing location.
2. Operating at the alternative site.
3. Refurbishing or replacing the damaged site.
4. Returning to normal operations once the damaged site has been refurbished.

Most organizations plan to recover only the critical systems at the alternative-processing site. These are the application systems needed to ensure continued business operations. If sufficient resources exist at the alternative site to run other systems, do not recover them until the critical systems are running.

See figure 4-2 for a schematic of an approach to developing a disaster recovery plan.

4.5.3 Insurance

For most businesses that rely heavily on computer processing, an effective disaster recovery plan is likely the only effective means of ensuring continued business survival following a major computer system disruption. However, it is possible to mitigate some of the financial loss through insurance coverage. Some examples of the kinds of insurance coverage available include:

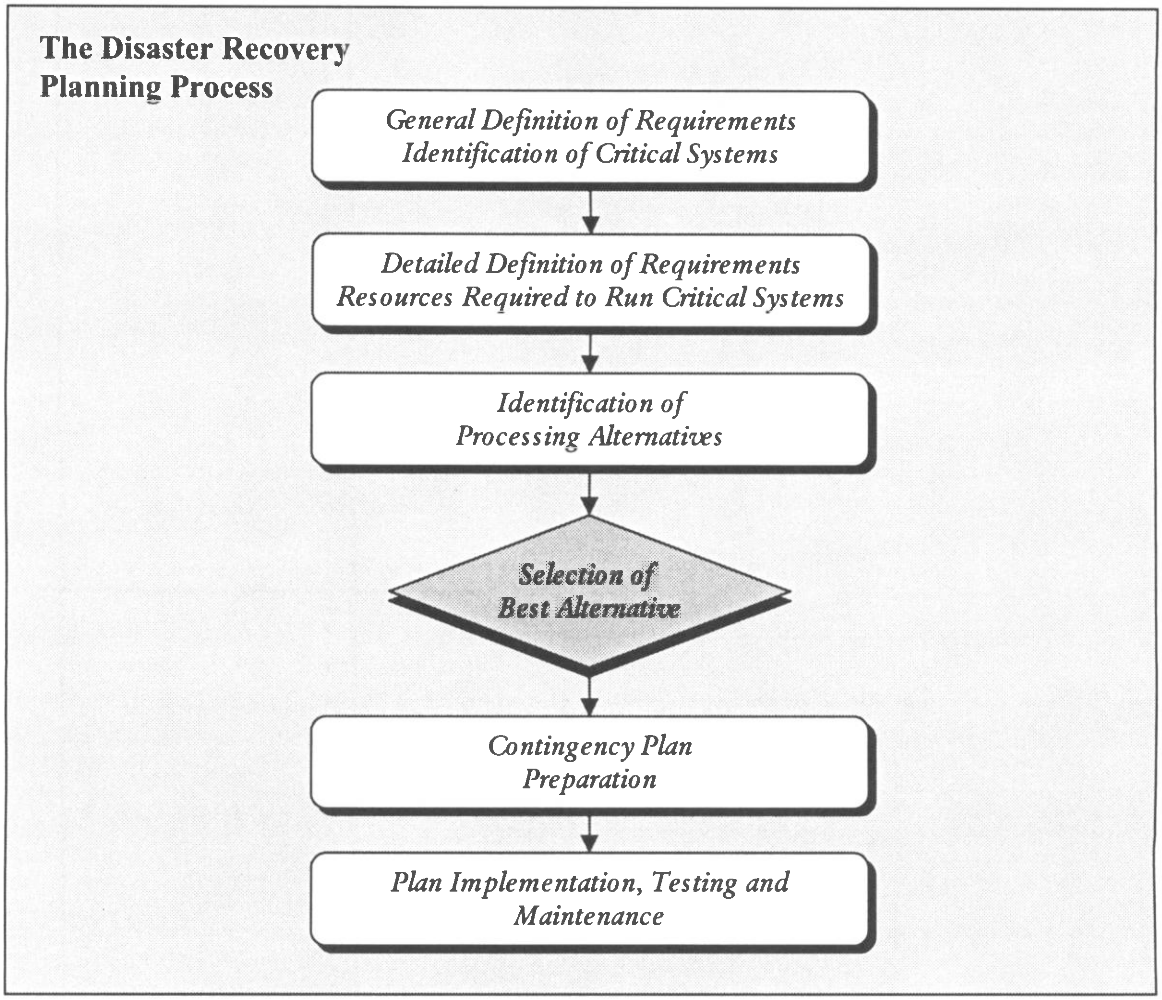


Figure 4-2. The Disaster Recovery Planning Process

- *Data processing equipment coverage:* These policies assist in defraying the cost of replacement computer hardware and air conditioning equipment. Some policies also cover the cost of removing the debris from covered equipment.
- *Data, computer programs, and media coverage:* These policies cover only data and programs in computer format, not hard copy. Organizations can take out insurance to cover the estimated potential loss if data and programs are destroyed.
- *Extra expense coverage:* These policies cover the extra expenses involved in continuing data processing operations if the equipment, air conditioning, or building housing the equipment is damaged.
- *Business interruption:* These policies cover the business losses incurred following a disaster in the computer department, subject to limits on the amount to be paid per day and a total amount payable.

- *Fidelity coverage:* These policies may cover costs associated with the unlawful acts of a dishonest employee. There are various new forms of crime coverage that may extend cover to certain acts by outsiders as well.

4.5.4 System Recovery for Microcomputers

Equipment failure for microcomputers generally is not a major concern for organizations, particularly compared with similar situations associated with larger computer systems; however, considering the dependency of many businesses on PCs and local area networks, it should be given more attention. If a PC fails, normally another machine is available or can be obtained with relative ease. Local area network (LAN) file servers and the communications gear associated with connecting LANs to private and public networks, including the Internet, may be highly specialized and take one or more days to replace and reconfigure. The biggest concerns are the potential loss of communications (which would, for example, cause a loss of electronic mail functions) and the loss of data stored on hard disk or diskettes.

Good PC and LAN security should be a priority in order to avoid situations requiring recovery. However, as noted earlier, disasters occur. Therefore, a regular policy of backing up hard disks is advisable. Consider using Norton Utilities (a system diagnostic-detection-recovery software) or a similar program because under certain conditions this specialized software enables the recovery of files that have been accidentally erased.

4.6 MANAGEMENT'S RESPONSIBILITIES IN A SECURITY PROGRAM

Management is responsible for providing protection for the organization's assets, including protection against dishonest employees and outside criminal acts. The information asset, administered in most organizations by the information systems or computer department, is as vital and vulnerable as any other asset. Although many organizations have invested heavily in the development of computerized systems to support their business operations, they have not invested sufficient effort to establish a security program that would properly protect that investment. Computer security is often neglected because of pressures to deal with day-to-day operating needs first, yet security can be *fundamental* to business survival.

You can implement effective security by identifying—

- The information in your organization that requires protection.
- The level of protection currently provided for that information.
- The risks and exposures that currently make that information vulnerable.

Using this approach, you can achieve a level of security that is appropriate to your organization's requirements. The objective is to provide sufficient security without going overboard and making security more complex than necessary. After taking the steps outlined in this chapter, your organization can implement a security program to address the exposures. This program should incorporate the development of policies, standards, guidelines, and procedures; the assignment of security responsibilities; and the monitoring of progress.

4.6.1 Policy, Standards, Guidelines and Procedures

It is generally unwise to assume that employees will act in a security-conscious manner particularly if the organization's expectations in this regard have never been communicated. Companies can communicate policies through the development and implementation of policy statements on computer security and should emphasize security and fraud awareness.

Effective policies must be short and succinct. If policies are too detailed and lengthy, they probably will not have the desired effect (especially with junior-level employees). For brevity, simply cross-reference the more-detailed standards, rather than attempting to include this material in the policy statement itself. The policy, standards, guidelines and procedures provide a framework for effective security in any organization.

Many organizations, in consultation with legal counsel, have determined that it is important to have employees sign a security and confidentiality agreement that defines the person's responsibility for safeguarding information in all forms. Indeed, many organizations have also developed agreements to be completed by contractors, vendors and temporary workers who require access to confidential and proprietary information.

4.6.2 The Security Function

Having recognized the importance of computer and information security to the organization, management must assign responsibility for this function. The person identified to take on the security function will usually be responsible for—

- Assisting in the development of policies, standards, guidelines, and procedures.
- Developing a formal security program to improve the level of security in accordance with management's expectations.
- Raising security and fraud awareness.
- Reporting on progress to senior management.
- Liaising with specialists in the event of crisis (for example, police, forensic accountants, computer forensics experts, and specialists in computer viruses).

Depending on the size of the organization, this may be either a full or part-time responsibility. Initially setting up the program probably will require a full-time position. One important function of the person or team charged with the computer security function is to regularly check the Internet for new information about the latest trends in fraud prevention and fraud techniques.

4.6.3 Policing

Once the security program is underway and the policy, standards, guidelines and procedures are in place, an organization must ensure compliance with expectations on an ongoing basis. This is a policing function.

Most organizations have an internal audit department that performs the policing function for controls that operate in other areas of the business. As such, internal audit may be an ideal candidate to become involved in testing compliance with corporate security expectations. Alternatively, external auditors or consultants can fill this role.

4.6.4 Evidence Recovery

If a security incident occurs, computer and security personnel may find they have different objectives. In an actual case in which a company's electronic mail servers suddenly reformatted their hard disk drives, the computer operations department saw as its objective repairing the damage and restoring email services within the company as quickly as possible. In contrast, the security people regarded the data center as a crime scene, and wanted to collect evidence to determine if the incident had been a technical accident or the deliberate act of a perpetrator. The two groups had to work together to ensure that technical personnel, who were assigned the task of restoring service (including outside consultants who were quickly brought in), would understand the importance of identifying any evidence of wrongdoing and call in the security people to gather and secure the evidence so that it would be admissible in court.

In cases where the crime scene is, in fact, the surface of a hard drive, the collection of evidence becomes critical. As with any other evidence, it is necessary to ensure that the process of collecting and safeguarding the evidence also preserves that evidence from any changes. Courts will not turn a blind eye when recovery technicians have made changes and later claim that the hard drive bears evidence of a crime. Under these circumstances, how is it possible to prove that the purported evidence of a crime wasn't planted to incriminate an innocent person? In complex or important cases, this task is often assigned to experts in the field of computer evidence recovery—a discipline known as *Computer Forensics.*

4.7 COMPUTER SECURITY CHECKLIST

Table 4.1, Computer Security Checklist is designed to assist CPAs in dealing with computer security in their organizations and in those of their clients. Generally, all *No* answers require investigation and follow-up, the results of which should be documented. Use the *Ref* column to cross-reference the checklist to any additional work papers.

The checklist is intended for general guidance and information only. Use of the checklist does not guarantee the adequacy of computer security, and it is not intended as a substitute for audit or similar procedures. If computer security is an especially vital concern or if computer fraud is suspected, seek the advice of a knowledgeable computer professional.

TABLE 4.1 COMPUTER SECURITY CHECKLIST

Computer Security Checklist	Yes	No	NA	Ref
1. Physical Security				
a. **Computer Room:** Most medium and larger organizations will have dedicated computer rooms for their mainframe computers or file servers. The following are basic questions to answer when looking at such a facility.	☐	☐	☐	___
• Are adequate fire detection and suppression systems in place (for example, does the computer room construction have a minimum one-hour fire resistance rating, in addition to smoke detectors, fire alarms, and sprinklers)?	☐	☐	☐	___
• Where sprinkler systems are in use, are adequate systems in place to protect against water damage (for example, underfloor water detectors, floor drains, waterproof equipment covers)?	☐	☐	☐	___
• Where power supplies are unreliable or the nature of processing is critical, are suitable precautions in place (for example, battery-equipped Uninterruptible Power Supplies (UPS) or backup generators, and surge protectors for PCs)?	☐	☐	☐	___
• Are appropriate environmental controls in place with respect to temperature, humidity and dust particles?	☐	☐	☐	___
• Is access to especially sensitive computer installations appropriately restricted (for example, through key locks, combination or cipher locks, or card access systems, along with access-control policies and procedures)?	☐	☐	☐	___
• Is overall physical computer security on the premises adequate?	☐	☐	☐	___
b. PCs and Workstations				
• Are PCs and workstations in areas where theft is a threat secured by cables, locks or other antitheft devices?	☐	☐	☐	___
• Are PCs and workstations secured with screen-saver programs that require passwords to unlock?	☐	☐	☐	___
2. Communications Security				
a. Is a user ID and password system in place?	☐	☐	☐	___
b. Is the ID and password system properly administered (for example, is the distribution of new IDs controlled, and are terminated users promptly deleted from the system)?	☐	☐	☐	___
c. Are users aware of the responsibilities associated with their password (for example, are they required to sign computer-use and confidentiality agreements, and are they instructed to maintain password secrecy and not to choose simplistic or easily guessed passwords)?	☐	☐	☐	___

(continued)

TABLE 4.1 *(continued)*

Computer Security Checklist	Yes	No	NA	Ref
d. Are passwords changed regularly (for example, every 90 days)?	☐	☐	☐	___
e. Does the system monitor and control use (for example, by restricting users to specific terminals or specific times, automatically logging-out inactive users, limiting the number of log-on attempts, and recording all usage for later follow-up and investigation if required)?	☐	☐	☐	___
f. For especially sensitive systems, is security to control remote access in place (for example, callback devices or one-time password devices)?	☐	☐	☐	___
g. Is a person or persons assigned to be responsible for the security function, including regularly checking Internet sources for information on fraud prevention and fraud techniques?	☐	☐	☐	___
3. Data Security				
a. Is access to on-line data limited to authorized individuals only, through built-in software restrictions or screening?	☐	☐	☐	___
b. For extremely sensitive data, has data encryption been considered as a security measure?	☐	☐	☐	___
c. Are data files stored on magnetic media (including all backups) kept in a physically secure location away from the computers, to which only authorized persons are allowed access?	☐	☐	☐	___
d. Are all printed reports subject to appropriate control and appropriate destruction (for example, shredding) when no longer required?	☐	☐	☐	___
4. Software Integrity				
a. Is access to production versions of all software tightly controlled by a production librarian or similar authorized person?	☐	☐	☐	___
b. Is access to all software programming code controlled so that programmers or others cannot subsequently alter tested and approved software?	☐	☐	☐	___
c. Are appropriate policies in place to guard against computer viruses (for example, prohibiting the installation of any copied or borrowed software, and screening all software with virus detection programs)?	☐	☐	☐	___
d. Are controls in place to ensure that the organization is not using unlicensed (pirated) software?	☐	☐	☐	___
5. Operations Security				
a. Do detailed operator instructions (for example, manuals) exist?	☐	☐	☐	___
b. Is computer activity logged and is any unusual operator activity investigated?	☐	☐	☐	___

TABLE 4.1 *(continued)*

Computer Security Checklist	Yes	No	NA	Ref
c. Are computer-operations personnel prohibited from altering the program code and the Job Control Language, which matches the program and data files to be run?	☐	☐	☐	___
d. Are all software and data storage media clearly and correctly labeled, including dates, to avoid errors?	☐	☐	☐	___
e. Are data files reconciled from run to run?	☐	☐	☐	___
f. Are all data storage media (including hard disk drives) erased (wiped clean) before being disposed of?	☐	☐	☐	___
6. System Recovery				
a. Are copies of all data files and software made on a regular basis (for example, weekly, with daily backups of transaction files)?	☐	☐	☐	___
b. Are guidelines in place to ensure that all employee work is saved to the network-server to ensure a complete backup of all data files?	☐	☐	☐	___
c. Is at least one backup copy of all data files and software stored off-site?	☐	☐	☐	___
d. Has training been provided and do written instructions exist for the disaster recovery procedures?	☐	☐	☐	___
e. In the case of catastrophic failure, do alternative processing arrangements exist?	☐	☐	☐	___
f. Have the backup plans been tested in a realistic simulation to provide assurance that they can work if needed?	☐	☐	☐	___
g. Is adequate insurance in place covering computer equipment, software, recovery expenses and business interruption?	☐	☐	☐	___

Internal Fraud

CHAPTER 5:

Internal Fraud

CHAPTER 5:

Internal Fraud

5.1 Asset Misappropriation from Within

As difficult as it is to believe, many experts are convinced that the worst threat to business is from the people who work there. Fraud committed against an organization by a perpetrator from within that organization is probably the most common form of fraud. Certainly it is the most widely recognized.

It is estimated that at least one-third of all employees steal to some degree. In retail organizations, shoplifters are responsible for only thirty percent of retail losses; employees steal the remainder. Probably the worst case of insider misappropriation is the infamous U.S. Savings and Loan scandal; the billions of dollars stolen by *trusted* insiders has no equal in history.

5.1.1 Classification of Fraud

Regardless of the industry, you can classify internal fraud in several different ways. One way is by the method of concealment, including on-book and off-book frauds.

On-Book Fraud

On-book fraud principally occurs within a business when an employee creates an audit trail (which is sometimes obscure) that inadvertently aids the employer in detection. Examples include phony vendors and ghost employees. On-book fraud is normally detected at the point of payment.

Off-Book Fraud

Off-book fraud occurs outside the accounting environment where no audit trail is likely to exist. Examples include bribery and kickbacks. If an employee receives a bribe for selecting a certain vendor, that payment would be made by the vendor and, therefore, would not be reflected on the books of the affected company. These frauds are detected in an indirect manner (that is, responding to other vendor complaints, investigating the life-style of the person receiving the bribes, and so on). If you suspect that an employee is receiving illicit payments, examining the employee's personal finances should prove this.

5.1.2 Cycles

You can classify fraud occurring within the business environment by one of the five cycles in the accounting system. These cycles are:

1. Sales and collection
2. Acquisition and payment

3. Payroll and personnel
4. Inventory and warehousing
5. Capital acquisition and repayment

All of these cycles flow through the cash account. Accordingly, cash misappropriation is discussed separately in this chapter. The following sections discuss the more common frauds occurring within each cycle.

5.2 Sales and Collection Cycle

The sales and collection cycle deals with the billing of goods or services to customers' accounts receivable and the collection of funds relating to those receivables.

5.2.1 Functions

The functions of the sales and collection cycle include:

- Receiving orders from customers
- Administering credit approvals
- Invoicing customers
- Collecting receivables
- Adjusting sales and receivables for allowances, returns and write-offs

5.2.2 Financial Statement Accounts

Sales revenue on the income statement and accounts receivable and cash on the balance sheet are affected by the sales and collection cycle. See Chapter 10 for further information on reducing the risk of financial statement fraud.

5.2.3 Perpetration

Frauds in the sales and collection cycle most commonly involve the theft of cash, the theft of other assets, and kickbacks to customers. It can also involve off-book fraud in a situation described as front-end fraud, that is, when an employee diverts company revenue before entering it on the books.

Theft of Cash

By far, the most common sales-cycle fraud is the theft of cash. The main schemes include: not recording sales, under-ringing sales, lapping, theft of funds from voids and returns, overbilling and keeping the difference, simple theft of cash, writing off receivables as uncollectible, and issuing bogus credit memoranda.

For example, in one lapping fraud, a cashier was able to misappropriate cash receipts totaling over $35,000 and cover the shortage by subsequent receipts. The prelisted receipts were not compared to the deposits by an independent person, allowing the fraud to go undetected over time. This scheme was eventually discovered as a result of a CPA following up on the clearing of deposits in transit listed on the year-end bank reconciliation.

Theft of Other Assets

These schemes include ordering and shipping company goods to the residence of the employee, and ordering goods for personal use.

Kickbacks to Customers

The most common schemes for kickbacks to customers include underbilling for merchandise and splitting the difference, and writing off receivables owed to the company for a fee.

Front-End Fraud

A front-end fraud occurs when a company's customers are improperly directed to take their business elsewhere, thereby depriving the company of profits it could otherwise have made. Another example is the receipt of a purchase rebate that is misappropriated and not deposited to the company's bank account.

5.2.4 Detection

Generally, CPAs can best detect frauds in the sales and collection cycle by analyzing cash or inventory, or both.

Theft of Cash and Front-End Fraud

Following are some methods for detecting the theft of cash and front-end fraud:

- Investigate customer complaints.
- Insist that customers examine receipts.
- Use statistical sampling of sales invoices.
- Compare receipts with deposits.
- Follow up on deposits in transit at the end of each period.
- Account for consecutive sales orders and cash register transactions.
- Compare volume of credit memos by period.
- Verify independently customers who don't pay.
- Examine gross margin by product.
- Use a computer to—
  - —Identify missing invoices by number.
  - —Match shipping documents, sales invoices and customer orders.
  - —Verify numerical sequence of documents.
  - —Analyze sales volume by employee.
  - —Match daily deposits with customer credits.

For example, in one fraud case, a CPA for a retail client noted a skip in the perpetual transaction count for one of the cash registers. During a one-year period an employee had destroyed sections of cash register tapes totaling $17,000. The irregularity was directly related to the company's failure to institute and maintain adequate internal controls and procedures over cash register tapes.

Theft of Other Assets

You can detect theft of other assets by using the following methods:

- Resolve customer disputes.
- Conduct periodic surprise inventory counts.
- Use statistical sampling of sales invoices, including examining the shipping address.
- Use a computer to—
  —Match sales invoices with customer orders.
  —Compare customer names and addresses with employee names and addresses.
  —Verify delivery addresses against addresses of customers.

Kickbacks to Customers

You can use one or a combination of the following to detect the common schemes in kickbacks to customers:

- Follow up on customer disputes.
- Conduct statistical sampling of sales invoices by contacting customers regarding prices and terms.
- Conduct computer analysis of—
  —Prices charged by product to customer.
  —Credit granting approval versus actual sales to customers.
  —Customer balances versus sales.
  —Customer balances versus length of time doing business with the customer.
  —Receivable write-offs.
  —Credit memos to customers.
  —Time between order and delivery.
  —Discounts to customers in descending volume of purchase.

5.2.5 Prevention

Employers can generally prevent sales and collection frauds by using adequate internal controls. More specifically, the following methods typically form part of an overall prevention strategy:

- Honesty testing
- Separation of duties
- Physical safeguards over assets
- Proper documentation
- Proper approvals
- Independent checks on performance

Honesty Testing

The legality of using certain kinds of honesty testing as part of the hiring process varies from jurisdiction to jurisdiction. For example, since the advent of the U.S. Polygraph Protection Act of 1988, generally it has been unlawful to require preemployment polygraphs of prospective employees. A number of companies have turned to pencil and paper honesty tests, which their designers tout as accurate.

Separation of Duties

Employers can prevent most frauds by properly segregating the custody, authorization, and record-keeping functions. In the case of sales and collections, it is important to separate the functions of credit granting and sales. In addition, the functions of sales, record keeping, and cash handling should also be separate.

Physical Safeguards over Assets

If assets and records have physical safeguards, misappropriation is much more difficult. In the area of computers, physical safeguards such as restricted access, locks, and similar controls are especially important.

Proper Documentation

Proper documentation requires adequate records, including prenumbered checks and invoices, to make fictitious entries more difficult. Documentation in sales and collections should include the following prenumbered documents:

- Sales orders
- Shipping documents
- Sales invoices
- Credit memos
- Remittance advices

Proper Approvals

Approval should be sought and evidenced before each of the following:

1. Granting credit
2. Allowing write-offs
3. Shipping goods

Independent Checks on Performance

In addition to a necessary independent review of employee adherence to internal controls, you should make the potential perpetrators aware that their performance is being monitored. Independent verification steps include reconciling bank accounts, audits and supervision.

5.2.6 Sales, Receivables and Receipts System

The sales, receivables and receipts system is the part of the accounting system that records a company's sales and revenue collections. Individuals can use false books and supporting documentation for sales, receivables and receipts to perpetrate a fraud on a company. This section covers three such methods:

1. Front-end fraud
2. False sales invoices
3. Lapping

Front-End Fraud

As discussed in section 5.2.3, employees may divert company revenues before that money ever reaches the sales, receivables and receipts system, thus circumventing the accounting system entirely. This is commonly called front-end fraud.

A front-end fraud occurs when company products are sold for cash, the sale and the receipt of the cash are not recorded, and the cash is diverted—usually, directly into the pocket of the perpetrator. A front-end fraud also occurs when a company's customers are improperly directed to take their business elsewhere, thus depriving the company of profits. Finally, a front-end fraud occurs when an employee receives and misappropriates special or unusual revenues and cost reductions, such as a purchase rebate.

The questions to address when investigating this kind of fraud are:

1. Do recorded sales represent all company sales? Where no sale has been recorded, there is nothing in the sales accounting system to *red-flag* an unpaid or overdue account. As a result, unrecorded sales are difficult to detect; however, actual inventory on hand has been depleted. Therefore, if the company has a good inventory accounting system, unrecorded sales may be detected.
2. Has the company unexpectedly lost some of its oldest and best customers?
3. Are all revenues recorded? Service businesses, such as parking lots, theatres and movie houses operate primarily with cash sales and have no inventory systems. Front-end frauds in these kinds of businesses, therefore, are extremely difficult to detect.

When allowed under local law, a review of a suspected perpetrator's personal bank accounts may reveal unexplained cash deposits, which could be important in establishing circumstantial evidence of front-end cash skimming. Otherwise use of the *net worth* approach may be necessary to establish that the suspected perpetrator has benefited.

Investigators should analyze the sales records and other supporting documents of the victim company for the period both before and after the assumed *occurrence* date of a front-end fraud. When possible, the investigators should interview customers as well.

"Taxes 'R Us" Case Study

Jane Brown and Jack Smith were cashiers who worked at a county tax office. Investigation revealed that, over a two-month period in 1997, thirteen individuals apparently paid tax for vehicle tags and did not receive an official receipt.

On a review of all the official receipts issued during this period of time it was found that:

1. The numerical continuity of the prenumbered receipts was complete; that is, all of the issued receipts were accounted for in the bureau's records.
2. There were no receipts to support the thirteen payments made by those individuals identified as exceptions.

The county tax office's banking records were then reviewed for the days on which people reportedly paid for their tags but did not receive a receipt. The review disclosed that the amount of cash and checks relating to the tax deposited to the county bank account totaled only the amount of receipts issued for that date.

Five of the individuals who reportedly paid for their tags, but were not issued an official receipt, paid by check. In the case of each of these five individuals, the checks were deposited to the county bank account, but the checks, upon deposit, were applied to cover actual receipts issued. With respect to those individuals who were known to have paid for their tags by check, but who did not receive an official receipt, it was noted that a like amount was included on the county tax office deposit slip.

During the same period, cash totaling $4,600 was deposited to the known bank accounts of Jane Brown. The source of that deposited cash was not identified.

Front-end fraud of this type is very difficult to detect. Larger frauds may be uncovered if the perpetrators become too greedy because the resulting unusually low daily deposits may highlight the problem. In fact, skimming of small amounts may be detected only through customer complaints: as in the case study, by the lack of an official receipt. This illustrates the need to thoroughly investigate similar complaints and any other irregularities.

False Sales Invoices

Employees can alter a company sales invoice to show a lower sale amount than what was actually received. They can misappropriate the difference between the real sale amount and the adjusted lower amount without the accounting system showing a *red flag*.

The questions to address when investigating this kind of fraud include:

1. Are recorded sales amounts the actual sales amounts?
2. Can customers confirm the sales?
3. Are sale amounts reasonable in the circumstances?

Investigators should obtain and examine all original copies of invoices and all the related books of original entry. Again, the investigator must become familiar with the accounting system in effect and understand the accused's position within that system. Did the accused have the necessary authority to perpetrate this crime? Did the accused have the opportunity?

"Ms. Wanda Cash" Case Study

Wanda Cash was the bookkeeper for Anytown Animal Center. She looked after all customer records including preparing bills and collecting payments. The owners of the business became suspicious when daily bank deposits were not as high as expected considering the level of business. Upon investigation by the owners, the police and forensic accountants, it was discovered that Wanda Cash, through altering sales invoices, had misappropriated approximately $11,700.

The investigation revealed that:

1. The 183 customer copies of sales invoices showed a total-charge amount higher than the total-charge amount recorded in the cash receipts journal. The customer copy of sales invoices indicated total charges to be higher by $2,579 than the amount recorded in the cash receipts journal.
2. The 549 office copies of the sales invoices indicated a total-charge amount higher than the total-charge amount recorded in the cash-receipts journal. The office copy total-charge amount was higher by $8,941 than the amount recorded in the cash-receipts journal.
3. Approximately 68 office-copy invoices were apparently altered so that the total charge after alteration balanced with the total charge recorded in the cash-receipts journal.

To uncover this fraud and measure its magnitude, investigators compared the following:

- Customer copies of invoices obtained by the investigating officer
- Office or accounting copies of the company's sales invoices
- Entries in the customer ledger cards and the cash-receipts journal

The result was that the amount of the total charge on the customer copies of sales invoices exceeded the amount of the total charge recorded in the cash-receipts journal by an aggregate amount of $2,579. An examination of these documents disclosed that in 54 separate cases the corresponding office copy of the invoice was altered so that the altered amount agreed to the total-charge amount recorded in the cash-receipts journal.

Investigators compared the office copies of the sales invoices with the total charge recorded for those invoices in the cash-receipts journal and found that the total charge amount on the office copy exceeded the total charge amount recorded in the cash receipts journal. In aggregate, the excess was $8,941.

This case illustrates the need for close supervision in small businesses, in which adequate division of duties is difficult to achieve.

Lapping

Lapping occurs when cash receipts from Customer A are misappropriated and the misappropriation is subsequently concealed by recording the receipt of monies from Customer B to the credit of Customer A (to the extent of the earlier misappropriation).

The questions to address when investigating this kind of fraud are as follows:

1. Are the amounts recorded as owing to the company actually still owing to the company?
2. Are deposits from *Peter* being used to cover *Paul's* debts?

To handle these questions, the investigator should understand the organization's system for receiving customer payments, making bank deposits, and preparing entries to customer accounts. The following is a guide to understanding an organization's account management.

1. Who first received the payments?
2. Who prepared the company bank deposit?
3. Who updated the customer accounts?
4. Has an individual *written off* any accounts?
5. Who approved the write-offs? (It is also often necessary to contact customers and obtain their records of payments, including paid checks and remittance advices.)
6. Do the customer's records show payment of specific invoices that are shown as unpaid in the victim company's records?

"Ms. B. A. Lapper" Case Study

Jones Transport Company operated a trucking terminal in Norcross, GA. Their accounts receivable clerk, Ms. B.A. Lapper, had been a loyal employee for over eight years. The terminal manager often complimented her for the extra effort she put into the business, evidenced by the amount of work she frequently took home. This employee was so loyal that her only time off was attributable to sickness.

Ms. Lapper was responsible for preparing the day's deposit to the bank and for preparing input to the computer systems for updating payments on accounts receivable. (The processing of the sales invoice as an account receivable was outside her control.) Every month the head office in Atlanta forwarded aged listings of accounts receivable to the manager's attention at the terminal. He gave the analysis to the accounts receivable clerk—Ms. Lapper—satisfied that the aged analysis was relatively current.

Investigators determined that Ms. Lapper had conducted a lapping scheme over a period of six years. The lap grew so large during this period that she had to take the aged receivable analysis home in the evenings, along with the *paid* and *unpaid* sales invoices. There, she would set aside invoices for payment during the next day to ensure a favorable aged receivable analysis in the following month. As the lap grew, the new cash receipts were no longer sufficient to cover the previously misappropriated funds. Accordingly, Ms. Lapper began to apply checks received from the larger customers of the company to cover up the already-paid sales invoices.

Investigators examined the known personal bank accounts of the accused and her husband. An amount of $35,000 was found deposited to these bank accounts over and above personal income during the relevant period.

Accounts Receivable Routines: Ms. Lapper's main function each day was to balance the cash with the pro-bills (sales invoices) and prepare a cash deposit for the bank in Norcross and a cash report for processing by the head-office computer. She would process all incoming checks from charge account customers by matching checks to the applicable pro-bill control copies and preparing a deposit for the bank in Norcross and a receivable report for the head office. She would present the deposit slips and receivable reports to the manager for his signature, along with the customer's checks and cash in an envelope.

The supporting documents were always in sealed and stapled envelopes for each report. The envelopes were not opened and verified by the manager. If the total of the bank deposit agreed with the total of the receivable report, he would sign the report. One copy of the report, the bank deposit slip, and pro-bills were then forwarded to the Atlanta head office, while a second copy of the report and the remittance copies of pro-bills were retained on file at the Norcross terminal.

Ms. Lapper would work on the company's *Accounts Receivable Aged Analysis,* a listing of all outstanding pro-bills prepared at the Atlanta head office, and would appear to question certain delinquent accounts for payment. She would often take the analysis home because she said she was too busy during the day to perform this function.

The Atlanta terminal manager would look at the receivable analysis printout and tell Ms. Lapper to question certain delinquent customer accounts, which she appeared to do. She would inform the manager of checks arriving after her contacts with the customer. For instance, in regard to the Best Quality Cheese account, she informed the manager that Best Quality was having serious problems converting to a computer accounting system and as a result had requested that Jones Transport be patient with the amount of old outstanding receivables.

Jones Transport hired a new person to replace Ms. Lapper when she became seriously ill. Her replacement began the collection work on the two largest charge-account customers, Best Quality Cheese and Anyco Inc. Successful collection of these accounts would immediately reduce the analysis' sixty- and ninety-day totals, which had become very high.

Customer Best Quality: Best Quality was advised that their pro-bills dated July and August were still outstanding on the receivable analysis. Ms. Brown asked Best Quality if they were having computer problems and the response was negative. Subsequently Best Quality informed Jones Transport that the pro-bills mentioned as outstanding were all paid by checks issued in July and August.

Jones Transport then examined copies of the reports around the dates of the Best Quality checks, together with check stubs and supporting pro-bills. Although the pro-bills that were paid with the Best Quality checks were all Best Quality, all were dated April and May. Jones Transport wondered if Best Quality had made an error, because their August check, which was paying July and August pro-bills, did not appear to apply to the pro-bills in the deposit that were all dated May and June. Best Quality responded that there was no error on their part, and they could not understand how there could be a mistake because they had attached all the applicable pro-bills with their remittances.

Customer Anyco: Jones Transport then called Anyco Inc. and asked when they would be paying certain outstanding pro-bills. Anyco indicated that these bills had been paid by checks that had been issued and received as paid. When Jones Transport checked their copies of the reports, they found that Anyco checks were deposited, but that the checks were applied to older Anyco pro-bills and other customer pro-bills and not to the pro-bills submitted by Anyco with its checks.

The outstanding pro-bills totaled about $47,000 at Best Quality and about $12,000 at Anyco. At this point Jones Transport recognized that the customer checks were not applied to the pro-bills as intended by the customer. Instead the checks were applied either to the customer's older pro-bills or to other customers' pro-bills. Further investigation revealed that these other customers were normally cash-paying customers.

Examination of the Amount of Money Due Jones Transport: To determine the correct amount of money owing to them by all their customers, Jones Transport communicated directly with each customer, based on their accounts receivable analysis. For each customer, Jones Transport prepared from their analysis a list of pro-bills by number, date, and amount that the customers had not paid and requested verification that the information concerning the outstanding pro-bills was accurate.

A reply made by all customers indicated that several pro-bills shown in the analysis of Jones Transport were, in fact, paid and were, therefore, not outstanding. This finding confirmed the evidence of the samples and the discussion by Jones Transport with both Best Quality and Anyco, that a customer's check was applied not to his current pro-bills as intended by the customer, but rather to a combination of the customer's older pro-bills and other customer's pro-bills that had been paid in cash.

From the information provided by the customers, the investigators determined that the dollar value of the pro-bills, which had been paid by these customers, was $115,132.

Jones Transport fell victim to a fraudulent scheme commonly called lapping. Cash and checks were received at the Hamilton terminal of Jones Transport and controlled by Ms. Lapper. The cash was removed from Jones Transport while the checks were applied to the pro-bills that were to have been paid by the cash. Consequently, the pro-bills remitted with the checks remained outstanding on the accounts-receivable analysis published at the end of each month.

As a result, the amount of the outstanding pro-bills, which Jones Transport found through direct communication with their customers to have been paid, represented that amount of the cash that had been misappropriated over the time period under investigation, that is, $115,132.

Victims most often detect lapping frauds through accounts-receivable reconciliations or confirmations, or both. Supervision is also important. Organizations can prevent lapping by appropriately dividing duties (for example, assigning someone other than the accounts receivable clerk the duty of handling cash receipts). You should also consider establishing a policy of mandatory vacations, which could be helpful.

5.3 Acquisition and Payment Cycle

The acquisition and payment cycle includes the procurement and payment of all goods and services except for payroll and capital acquisitions. This cycle is especially vulnerable to fraudulent transactions because this is the point where funds flow out of an entity.

5.3.1 Functions

The functions of the acquisition and payment cycle include:

- Processing purchase orders and dealing with vendors.
- Receiving and recording goods and services.
- Accounting for the liability of items or services purchased.
- Processing and recording cash disbursements.

5.3.2 Financial Statements Accounts

Balance Sheet

The following balance sheet accounts are affected by the acquisition and payment cycle:

- Cash
- Inventories
- Prepaid expenses
- Land
- Buildings
- Equipment
- Accumulated depreciation
- Accounts payable
- Deferred taxes
- Other payables

Income Statement

The following income statement accounts are affected by the acquisition and payment cycle:

- Cost of goods sold
- Advertising expenses
- Travel and entertainment expenses
- Miscellaneous expenses
- Income tax expenses
- Professional fees
- All expense accounts
- Gains and losses on sales of assets

5.3.3 Perpetration

By far the most common fraud in the acquisition and payment cycle involves the purchasing agent (buyer), who is especially vulnerable to the temptation of accepting kickbacks and gifts from outside vendors.

One study revealed that companies who caught employees accepting small gifts were hesitant to discharge their employees. Two percent suspended the employees, while only 12 percent fired them. Sixty-six percent reprimanded the employees and made them return the gifts.

There are three general kinds of acquisition and payment-cycle frauds:

1. The buyer-employee acts alone, and without outside assistance.
2. The vendor acts alone.
3. The buyer acts in collusion with the vendor. As is the case with other methods of prevention and detection, the collusion between both parties is the most difficult to prevent and detect.

Buyer Acting Alone

Noncollusive purchasing frauds usually involve the use of a nominee entity, commonly called a shell company, that is, an apparent third party owned by the buyer. Examples include the use of a nominee entity to submit fictitious invoices (the most common fraud), or to order goods for personal use.

Shell company schemes can be quite sophisticated using bank accounts, corporate filings, and mail drops to assist in the fraud. One common shell company failing is using a post office box rather than a street address. The post office box address has come to be recognized as a red flag.

In one case, a 61-year-old employee of a major department store was indicted for allegedly stealing $2 million from the company. His responsibilities included leasing buildings to house the retailer's stores. On twenty-two leases over a two-year period, through a nominee company, he altered leases to receive overpayments, and forged invoices billing the company for fictitious legal and building services.

In another example, an executive was indicted for defrauding a large cosmetics company of $1.1 million over four years. During this period, he allegedly approved more than 150 vendor invoices for services that were never rendered in connection with a newsletter the company was going to publish. The executive (whose salary was $124,000 per year) helped set up two nominee printing companies, which bilked his employer with the fraudulent invoices.

Finally, a director of customer-service technology was able to defraud his employer of over $2 million in one year by taking advantage of defects in internal control. The fraudster set up a legitimate agreement with a legitimate vendor to provide certain equipment. Then he set up a fake distributorship and told the vendor the company would purchase only from this one distributor. The vendor was content to have the business and proceeded to invoice the distributor. The fraudster, through his nominee distributorship, then inflated the invoices and billed them to his employer. The fraud was possible because the employee had the authority to set up the agreement, and to approve invoices for payment. The fraud was discovered by a manager who thought it was strange that the employee was delivering the invoices to accounts payable by hand.

Buyer and Vendor in Collusion

Nearly all collusion between buyer and vendor involves some form of secret commission or kickback from the vendor to the buyer. In these cases, secret benefits are given by a vendor in order to *buy* business, or are requested by the buyer for direct financial benefit. Collusion fraud often involves more than one kind of scheme perpetrated over time. Of course, there is always the question of who took the initiative, that is, the buyer or the vendor.

For example, one case started out involving inferior goods and later graduated to inflated invoices. A county purchasing agent was responsible for acquiring a long list of janitorial supplies, including mops, pails, soap, plywood, rakes, and paper goods. Area paper jobbers—experienced connivers—approached the purchasing agent with a deal. "Without changing our invoice price," they told him, "if you agree, we can deliver a cheaper brand of paper towels. Half the extra is for us; the other half is for you." Once the purchasing agent accepted a lesser brand, the vendor began squeezing for more by raising the price on the invoice and billing for five times the amount of merchandise actually shipped.

Monetary payments are not the only benefit that can be offered. Other common ways of corrupting a buyer include products or services; gifts, trips, or sex; promises of subsequent employment; reduced prices for personal items; and employment of friends or relatives.

Vendor Acting Alone

Common schemes used by vendors include product substitutions, billing for work not performed or services not provided, undershipping, padding overhead charges, and courtesy billings.

5.3.4 Detection

Because of the difficulty of detection, fraud awareness and prevention is the best policy, that is, know your vendors, and have an effective tendering process for all contracts. Fraud in procurement contracts always poses special problems, and detection is difficult. Common red flags include sole source contracts, unhappy purchasing agents, significant price changes or changed orders (especially after a contract is awarded), and vendor complaints.

In one case detected through vendor complaints, a buyer with six years' seniority obtained purchase requisitions from various departments at his plant. He then created a nominee company and placed orders with this firm. The nominee company would place real orders with a legitimate vendor and have them ship the merchandise to his employer. The merchandise would be billed through the buyer's company at 150 percent of the real amount. The scheme was unraveled when the buyer failed to pay one of the vendors, who then complained to the buyer's employer.

Sometimes you can also detect schemes through a computer analysis of the following:

- Timing of bids
- Patterns of bids
- Amount of work performed by vendors
- Patterns of hiring new vendors
- Vendors with post-office-box addresses

In an example involving post-office-box addresses, a junior buyer, who had been with his company for two years, created five nominee companies that he then placed on an approved vendor list. Thereafter, he did business with these phony companies, placing various orders with them. The scheme was unraveled when the auditors noticed that these particular vendors all had post-office boxes for addresses and were not listed in the telephone book. The amount of money lost was in excess of $250,000 over a period of more than a year.

If you suspect that a buyer and vendor are in collusion, consider the following items:

- Assessment of the tender process, if any
- Patterns of business and bids
- Noncompetitive pricing
- Products of inferior quality
- Buying unnecessary goods or services
- Lack of competitive bidding

5.3.5 Prevention—Key Controls

As previously noted, prevention of procurement fraud can be achieved best through fraud awareness, effective tendering and budgeting, and knowledge of your vendors. Other prevention controls include proper documentation, approvals, and segregation of duties.

Proper documentation includes prenumbered purchase requisitions, purchase orders, receiving reports, and checks. Proper approvals should include detailed background information on the vendor; ideally, purchase contracts should include a right-of-audit-access clause to the vendor's books. In addition, conduct both irregularly scheduled audits of the purchasing function as well as assessments of the performance and happiness of the purchasing agent.

5.3.6 Prevention—Policies

Organizations should have established prevention and detection policies. The following are some policies to consider implementing.

Accepting Gifts

The following is a sample policy statement covering the acceptance of gifts and gratuities:

> "Employees, and members of their immediate families, should not accept gifts, favors or entertainment that might create or appear to create a favored position for someone doing business with the company. Advertising novelties or trinkets are not considered as gifts and are excluded from these restrictions.
>
> Gifts that are received by an employee should be returned to the donor and may be accompanied with a copy of this policy. Perishable gifts should be donated to a charitable organization and the donor notified of the action taken.
>
> It is not the intent of this policy to preclude the acceptance by the company's employees of occasional meals or refreshments that are provided in the normal course of business-work relationships, with other individuals. Discretion must be used, however, in the limited acceptance of meals, refreshments or incidental hospitality to avoid situations that could create a conflict of interest or appear to do so."

Providing Gifts

The following is a sample policy statement covering the giving of gifts:

> "Occasionally, it may be appropriate for employees, acting for the company, to provide people outside the company with promotional items, meals, refreshments, transportation, lodgings or incidental hospitality. Expenditures for such purposes should be moderate and should be done only within the framework of good taste. All expenditures are subject to the overall company policy that an employee shall avoid constituting improper influence over others."

Use of Hotlines

You should study the feasibility of installing hotlines to monitor complaints by employees and other vendors. Make sure the hotline staff is not associated with either the purchasing or payment functions. Failure to take this precaution could result in the fraudster receiving the whistle blower's call.

Disposition of Materials

The purchasing department normally should not be in charge of disposing of obsolete inventory, scrap, or fixed assets.

Rotation of Jobs

Rotate buyers frequently within a department to keep them from getting too close to vendors. In addition, enforce a mandatory vacation policy.

Competition in Bidding

Ensure that bidding policies and procedures are thoroughly reviewed. Whenever possible, enforce competitive bidding.

Compensation of Buyers

Buyers should be well paid to reduce the motives and rationalizations for fraud.

5.3.7 Purchasing, Payables and Collection Systems

The purchasing, payables, and collection systems are part of the accounting systems that record a company's purchases and expense payments. Employees can falsify books and supporting documentation for purchases, payables and collections to perpetrate a fraud on their employing company. This section covers three categories of perpetrating fraud:

1. False expense reports
2. False supplier invoices
3. Other false information

False Expense Reports

Expense reports prepared and submitted to the company for payment are false if they include any of the following:

- Overstated items
- Fictitious items
- Duplicate items

An employee could use a company credit card for personal items. If the company pays the entire amount of an employee's account, that employee may be committing a fraud. Ultimately, the answer depends on the first accountability for the disbursements.

Address the following questions when investigating this kind of fraud:

1. Is the expense item an allowable business-related expense? It is necessary to determine the company's policy regarding allowable business expenses.
2. Is the expense amount the actual amount incurred? It is necessary to obtain the suppliers' copies of the original expense vouchers and compare them with those submitted in support of the expense report.
3. Is the expense ultimately charged directly to the business? If yes, is there evidence of any reimbursement?

It is also necessary to understand the approval and payment system in effect. Who approved the expense reports? How were the expense reports categorized in the accounting records? Were the expense reports adjusted at a later date to reflect those items of a personal nature? Was there any pattern in the submission, approval or recording (or any combination thereof) of the fraudulent expense reports?

"Manny Miles" Case Study

Manny Miles had been the Business Administrator and Secretary-Treasurer for The County Hospital since shortly after it was formed in 1983. In addition to overseeing the administration of the hospital and its 145 employees, Miles' duties included preparing budgets. He had check-signing authority and payment approval for the hospital's annual budget of about $5 million.

The governing body of the hospital consisted of a board comprised of twelve members; eight were elected and four were appointed as representatives of the county. In 1993, the board members hired Dr. Jane Wilson as Medical Officer. Almost immediately Miles and Wilson developed a severe personality conflict; accusations and negative feedback caused a division between the personnel of the hospital and members of the board. Attempts to terminate Dr. Wilson's services failed due to the intervention of the hospital board members on her behalf. The hospital conducted studies to improve conditions but never implemented any recommendations.

In mid-1996, during its audit, the auditors found irregularities in travel claims submitted by Manny Miles, and the hospital referred the matter to the police for investigation. In December 1996, and January 1997, the police executed search warrants not only on the hospital but also on the residence of Manny Miles. They seized the hospital's financial records along with Miles' personal banking records.

Examination of the records revealed that from 1993 to 1996, Miles had continually made claims for travel expenses while using a hospital car. Additionally, he claimed mileage from both the hospital and the county for the same trips. Furthermore Miles had used his hospital credit card to repair his own vehicle and purchase numerous personal items, including restaurant meals on weekends, when he was not working. The card was in Miles' name but the hospital paid the bills.

As business administrator, Miles could approve his own expenditures and authorize the checks. To conceal his spending, Miles had authorized the listing of these expenditures in the hospital's financial records under other categories. Invoices were missing for some checks issued and for credit-card expenditures. The financial records of the hospital did not show any reimbursement by Miles to cover the vast majority of his personal purchases, although on several occasions he had made restitution for small purchases on the hospital card.

The Manny Miles case shows that independent approval and division of duties is essential in the payment of all travel claims and other expenses. Employees should not be able to approve their own expense reports. In addition, check signers should not be the same people approving expense reports.

False Supplier Invoices

Suppliers' invoices prepared and submitted for payment to the company are false if either:

1. No goods have been delivered or services rendered
2. The quantity or value (or both) of the goods are inflated

The delivery of goods or services to a location other than a business location (for the use and benefit of the perpetrator) is a common technique, as is the payment to a *friendly* supplier when no goods or services were actually provided. Payments of inflated amounts to suppliers often reflect the existence of secret commissions.

Address the following questions when investigating this kind of fraud:

1. Were goods and services actually provided? Find out, first, whether the supplier company actually exists and next, whether any goods or services were in fact provided. If they were provided, determine to whom.
2. Did the company receive the benefit? It is often necessary to obtain the bills of lading, that is, the freight companies' proof-of-delivery slip, to confirm where the goods and services were delivered.
3. What was the approval and payment system? As with false expense reports, you should understand the approval and payment system.

"Credit To You Inc." Case Study

In January 1993, Jones and Smith signed an agreement to start Smith Construction, a business that primarily consisted of erecting service stations. It was agreed that Smith would provide the financing while, for a salary of $600 per week plus expenses, Jones would manage and operate the business. Smith and Jones were to share equally any profits from the business. The business progressed well and showed a profit for the first three years.

Smith did not take an active part in the construction business, as he continued to operate his own plastering company. Smith Construction operated as a division of Smith Plastering Corp. Smith initially invested $42,000 as capital to start the construction business, and as sole signing officer, would attend the Smith Construction office regularly to sign checks, some of which were blank when signed.

Jones tendered and obtained contracts, hired subcontractors, hired and fired employees and purchased the goods necessary to operate the business, without interference from Smith. Jones could also purchase material he required for himself through the construction business and charge these amounts to himself on the business books as a form of salary.

Smith was aware that over the years Jones had erected a barn on his farm, renovated other buildings including his residence, and continued to operate the farm. Jones informed Smith that he had obtained a grant from the government of $300,000 to finance these endeavors.

In 1998, Smith Construction had difficulty paying its suppliers (creditors) and was eventually forced into bankruptcy by creditors in June 1998. The company's debts exceeded $300,000. Jones gave no explanation for the shortage of funds except to say that he had miscalculated the actual cost of various construction jobs. An examination of Smith Construction's books, canceled checks and available supporting documentation revealed that Jones had defrauded Smith Construction of $861,000 by various means.

As general manager, Jones was responsible for the day-to-day operations and in this capacity, he was afforded a degree of trust. At the same time, Smith, the absentee owner, retained signing authority over all checks and, thus, thought he had control over all policy decisions.

In his private life as a farmer, Jones incurred debts with suppliers who also dealt with him as general manager of Smith Construction. Jones personally owed one of these suppliers, Credit To You Inc., more than $25,000. In June 1997, Jones purchased a $12.30 item, documented by the supplier invoice made out in pencil. Later, the penciled information on this invoice was erased. Information was typed onto the invoice, indicating instead that the company, Smith Construction, had purchased $9,500 worth of material for a job then in progress. On the strength of this typed document, Smith signed a check for $9,500 to the supplier, believing, of course, that the disbursement was for the benefit of Smith Construction. When the supplier received the check, on Jones' instructions, he credited Jones' personal account, reducing the debt to $15,500. This altered document was the prelude to a fraud of more than $861,000.

The alteration of documents (erasures, stricken information, or both) is at times the only indication of a fraud as it can disclose a change of mind (intent) by the person making the entry. Such alterations frequently occur in the earlier stages of a fraud as the perpetrator has yet to perfect the scheme.

Acme Products Inc. invoiced Smith Construction for the sale of roof trusses, with delivery scheduled for a gas station being built by Smith Construction. However, a description of the route to Jones' farm appeared on the back of the invoice. The building of Jones' barn required roof trusses. A review of the bill of lading confirmed the redirection.

Investigators can also review delivery instructions as another technique for identifying fraudulent transactions.

Other False Information

A business receives vast amounts of information, and subject to the existing systems of internal control, relies on it in making decisions, initiating, executing and recording transactions. If this information is false, a business can be deceived, resulting in deprivation of some sort and hence the company is put at economic risk.

Examples of false information that businesses may rely on include:

- False financial statements (See Chapter 10 for further information on financial statement fraud.)
- Overstated accounts receivable listings
- Overstated statements of income and net worth
- False general journal entries
- Altered internal company records
- Fictitious customer credit information
- False asset valuations

Address the following questions when investigating this kind of fraud:

1. Is the summary information presented (accounts receivable listings, financial statements) consistent with the underlying books and records, and are the real assets on hand? It is necessary to determine the representation made by the person or entity under investigation and the understanding reached between that person or entity and the victim. Once accomplished, you can examine the books and records supporting the summary financial information in question from the appropriate perspective.
2. Have the correct authorities properly approved entries in the general ledger? Are the entries appropriate and consistent with the facts?
3. Can customers confirm transactions?

To address the second and third questions above, you should understand the accounting systems in effect. Also, you should contact third parties to review and discuss with them their books and records, and then compare that information to the victim's information.

"Ms. I. O. Much" Case Study

Ms. I.O. Much was the office manager of Anyco Inc. from May 1995 to May 1998. As office manager, Ms. Much, together with the general manager and president of the company, had check-signing authority for the company payroll account.

While Ms. Much was office manager, the company's auditors frequently had difficulty completing their audit work primarily because of the poorly maintained books and records. Finally, Ms. Much was replaced with a new office manager, who found irregularities in the company's bank reconciliations. After the company, police, and forensic accountants completed an investigation, they determined that I.O. Much received unauthorized payments from the company totaling at least $11,195. These payments were covered up in a variety of ways.

After examining banking records for the payroll account of Anyco Inc., investigators noted all checks payable to the order of I.O. Much. They found that eight checks totaling $9,126 were paid to I.O. Much but were not recorded in the payroll journal.

June 15, 1997: A check dated June 15, 1997, in the amount of $2,500 was paid to I.O. Much but not recorded. Attached to the December bank statement was a note dated June 15, 1997, which stated, "This is to certify that I.O. Much received a loan of $2,500 from Anyco Limited to be repaid before the end of the year." The bottom of the note had a legend stating "paid Dec. 28/97." It appeared that no record had been made of this apparent loan transaction until December 1997.

A review of relevant accounting records disclosed that on December 28, 1997, a deposit of $2,500 was made to the Anyco general bank account. The deposit slip for this $2,500 showed that the deposit consisted of three checks, as follows: $350, $178, and $1,971. The sources of the three checks noted on the deposit slip appeared to be as follows:

1. William Smith—$350: A check was issued to Anyco on the account of William Smith, dated September 8, 1997. The current office manager at Anyco stated that this check was a repayment to Anyco as a result of an over-advance of funds to Smith, an Anyco employee.
2. Anybank—$178: A check was issued from Anybank to Anyco Limited.
3. Bank draft—$1,971: The check was a bank draft purchased from Otherbank. When this deposit was recorded in Anyco's records, someone apparently recorded it as a reduction of the company loan to I.O. Much. This loan was reflected in the books as having been advanced and repaid in the same month, that is, December 1997.

March 1, 1998: A check dated March 1, 1998, in the amount of $2,500 was paid to I.O. Much but not recorded in the payroll journal. It appeared that a journal entry was prepared to record this check. This journal entry suggested that the $2,500 was paid with respect to five different accounts as follows:

1. Account #99-6, salespeople's salaries, Boston
2. Account #99-2, salespeople's salaries, Dallas
3. Account #99-7, salespeople's salaries, Washington, D.C.
4. Account #199-12, delivery salaries, New York
5. Account #99-8, salespeople's salaries, Seattle

The journal indicated that this entry was "to record checks cashed but not recorded or deposited." The only check apparently not recorded in March 1997 was check #2000 for $2,500 payable to I.O. Much.

It is significant that the checks paid to I.O. Much in 1997 and 1998, which were not noted in the payroll journal, were not available in the corporate records. Investigators obtained copies of these checks from the microfilm files at Anybank.

A review of the payroll records indicated two apparent discrepancies related to I.O. Much. The April 7, 1997, payroll records indicated "income tax withheld" of $200 more than apparently had been withheld from I.O. Much's pay. Similarly on August 11, 1997, payroll records indicated $1,000 more income tax withheld than apparently had been withheld to date. In that time period an offsetting adjustment was made to the net pay figure, thereby indicating that the net amount of money paid to I.O. Much was $1,000 less than apparently had been paid to her at that time.

The effect of these adjustments was an apparent benefit to I.O. Much of $1,200. Her W2 for the year ended December 31, 1997, indicated that she paid $1,200 more income tax than she had actually paid. The Anyco Limited employee deduction account was not reconciled at the time of the investigation, and thus it was not readily apparent how the $1,200 tax benefit was accounted for in the company's books.

While the amounts involved were not terribly large, this case points out a number of internal control weaknesses that can result in fraud, including lack of supervision, inadequate division of duties, and failure to perform appropriate accounting reconciliations.

5.4 Payroll and Personnel Cycle

The payroll and personnel cycle handles the hiring, firing, and payment of employees, along with timekeeping, expense-account and travel reimbursements, and insurance matters.

The hiring function can play an important role in reducing the risk of potential fraud through the careful vetting of employment applications. Adding an employee whose resumé is not truthful is opening the business's door to a potential fraudster.

5.4.1 Functions

The functions of the payroll and personnel cycle are as follows:

1. Personnel and employment
2. Preparation of timekeeping and payroll
3. Payment of payroll
4. Payment of payroll taxes and other withholdings
5. Reimbursements of expense accounts and travel expenses
6. Processing and payment of employee insurance, pension withholdings, and other employee benefits

5.4.2 Financial Statement Accounts

Balance Sheet

The following balance sheet accounts are affected by the payroll and personnel cycle (see Chapter 10 for further information on financial statement fraud):

1. Cash
2. Salaries payable
3. Payroll taxes payable
4. Other withholdings payable

Income Statement

The following income statement accounts are affected by the payroll and personnel cycle:

1. Travel and entertainment expenses
2. Salary and commissions expenses
3. Payroll tax expenses
4. Medical and insurance expenses

5.4.3 Perpetration

Payroll is particularly ripe for internal fraud. Common schemes include nonexistent or ghost employees, fictitious hours and overtime abuses, overstating expense accounts, and fictitious or overstated medical claims.

In one case, approximately one month after the payroll check date, Mr. Smith attempted to pick up his check from Ms. Doe, who was responsible for all departmental check distributions. Ms. Doe stated that the check was lost and that she would process the paper work necessary to obtain a new check. She then entered false payroll data in order to generate the check. Within a few weeks, Mr. Smith received a new check. However, upon reviewing his year-to-date earnings, he discovered that the lost check amount was included in his earned income. When confronted with the situation, Ms. Doe admitted to her supervisor that she had forged Mr. Smith's name and cashed the check for personal reasons. Ms. Doe, who had been with the company for seven years, had her employment terminated.

Expense accounts are easily and frequently abused. For example, the president of a subsidiary submitted requests for business travel and entertainment advances with the parent company. The chief accountant issued the checks for the requested advances. After one-and-a-half years, the president had not repaid the advances. When pressed, he could not support the advances with proper business receipts. He confessed that he had none. The president who had ten years of service, had his employment terminated. The amount involved was $120,000.

5.4.4 Detection

Organizations typically discover ghost employees when payroll checks are hand-delivered, and extra checks are left. For businesses employing vigorous payroll fraud detection procedures, investigators can perform significant computer and statistical analysis. For example, time card approvals, which are the same as signatures and endorsements on checks, can provide items for further investigation. Computer-generated detection methods could indicate:

- Payments to employees not on the master lists
- Payments to employees versus those not authorized for payment
- Write-offs of employee accounts
- Duplicate payments to employees
- Overtime by employee
- Password use during vacation
- Social security numbers listed in descending or ascending order
- Employees with no withholding
- Each kind of withholding in descending order
- Salary expenses in descending order
- Hours worked in descending order
- Time-card hours versus authorized job orders
- Hours worked by employee by pay period
- Pay rates in descending order
- Dates of employment versus authorized dates of payment
- Travel reimbursement by employee overtime
- Travel reimbursement compared to other employees

- Travel reimbursement for specific function by employee
- Travel reimbursements by kind of expense, that is, rental car, hotel, airfare, and so on
- Date of travel reimbursements compared to dates employee worked
- Numerical sequence of employee travel reimbursements

5.4.5 Prevention

Proper Documentation

Proper documentation for payroll purposes includes time cards for appropriate employees, prenumbered travel reimbursement forms and payroll checks, and verification of medical services.

Proper Approval

Proper approval includes hours worked and wage rates, hiring and terminations, overtime, medical benefits, and travel allowances.

Separation of Duties

At a minimum, you should consider separating the following duties to reduce the possibility of one employee acting alone.

- Accounting for hours worked and processing checks
- Processing and distributing paychecks
- Hiring and firing from timekeeping
- Claims processing, approval, and payment
- Travel expense approval and payment

Independent Verification

Independent verification is especially important for preventing payroll and personnel fraud, and includes the following:

- Using time clocks wherever possible, and verifying the hours worked against the clock
- Ensuring hours worked are approved by someone other than the employee
- Conducting surprise audits of the personnel and payment cycle

5.5 Inventory and Warehousing Cycle

The inventory and warehousing cycle includes functions relating to the purchase and warehousing of merchandise for manufacture and resale. Because of the volume of activity and funds involved, fraud represents a significant risk.

5.5.1 Functions

The functions of the inventory and warehousing cycle include:

- Processing purchase requisitions.
- Receiving raw materials and finished goods.
- Storing raw materials and finished goods.
- Cost accounting.
- Processing goods for shipment.
- Shipping finished goods.

5.5.2 Financial Statement Accounts

Inventories on the balance sheet and cost of goods sold on the income statement are affected by the inventory and warehousing cycle. (See Chapter 10 for further information on financial statement fraud.)

5.5.3 Perpetration

The more common frauds in the inventory and warehousing cycle include: ordering unneeded inventory, appropriating inventory for personal use, theft of inventory and scrap proceeds, and charging embezzlements to inventory.

For example, a loading-dock employee and delivery-route driver were able to steal $300,000 of inventory through collusion over a six-month period. The load sheets at the dock were either not filled out or inaccurately completed by both employees (control procedures required the dock employee and route driver to verify the quantities loaded and sign a load sheet). The products were transported to an independent distributor and subsequently sold. The defalcation surfaced when outside sources informed the company that certain products were being stolen as the result of collusion between particular employees and an independent distributor.

In a case involving a theft of inventory, an inventory records supervisor and a security guard colluded to steal $400,000 from a jewelry warehouse over a two-year period. The security guard stole the merchandise, and the supervisor concealed the theft by manipulating inventory records. An undercover investigator, who was hired because of a significant increase in year-end inventory shortages, eventually discovered the theft. After this experience, and following a consultant's recommendation, the company started to perform surprise physical inventories at varied times during the year.

5.5.4 Detection

The three primary ways for detecting inventory and warehousing frauds are: statistical sampling of documents, computer analysis, and physical counts.

Statistical sampling includes looking for inconsistencies and discrepancies in purchase requisitions, as well as receiving reports, perpetual inventory records, raw material requisitions, shipping documents, job-cost sheets and similar documents.

Computer analysis includes identifying the following items:

- Purchases by item
- Purchases by vendor
- Inventory levels by specific kinds
- Inventory shipped by address
- Costs per item over time
- Direct labor per inventory item
- Direct materials per inventory item
- Overhead per inventory item
- Disposals followed by reorders
- Shortages by inventory item
- Shipments by address

5.5.5 Prevention

Prevention is critically important in the case of inventory and warehousing fraud because of the amounts of money involved and the relative ease with which this kind of fraud can be concealed. Prevention includes: receiving reports, keeping perpetual records, using prenumbered and controlled requisitions, raw material requisitions, shipping documents, and keeping job-cost sheets.

Someone independent of the purchase or warehousing function should handle approvals of purchasing and disbursement of inventory.

Separation of duties becomes critical in preventing this kind of fraud. Authorization to purchase should be handled by someone not performing the warehousing function. Someone other than the individual responsible for inventory should handle the receipt of inventory.

Independent checks on performance are also important prevention measures. Someone independent of the purchasing or warehousing functions should conduct the physical observation of inventory.

Physical safeguards include ensuring that merchandise is physically locked and guarded, and that entry is limited to authorized personnel.

5.6 Capital Acquisition and Repayment Cycle

The capital acquisition and repayment cycle, sometimes referred to as the financing cycle, includes borrowing money and accounting for the debt of an entity.

5.6.1 Functions

The functions of the capital acquisition and repayment cycle include: borrowing funds and accounting for debt, accounting for and paying interest, accounting for and paying dividends, accounting for stock transactions, and equity financing.

5.6.2 Financial Statement Accounts

The following balance sheet and income statements are most often associated with the capital acquisitions and repayment cycle (see Chapter 10 for further information on financial statement fraud):

- Cash
- Notes
- Mortgages
- Accrued interest
- Capital stock
- Capital in excess of par value
- Retained earnings
- Dividends
- Dividends payable
- Interest expense

5.6.3 Perpetration

The common schemes in this cycle include borrowing for personal use, misapplication of interest income, and theft of loan and stock proceeds.

In one case, a factoring company obtained a credit facility from a regional bank to fund the purchase of qualified assets, primarily accounts receivable. The vice president of the company, in collusion with a customer, purchased fictitious accounts receivables with the proceeds of the credit facility. Part of the purchase proceeds was wired to offshore bank accounts beneficially owned by the vice president. The activity was discovered when the bank manager reviewed the bank account of the factoring company and saw wire transfers made to Caribbean tax havens. He hired forensic accountants who discovered the bank had been defrauded of $9.5 million over a two-year period.

5.6.4 Detection

Most frauds in the capital acquisition and repayment cycle involve tracing the proceeds of loans to ensure that all of the proceeds go to the benefit of the company. This can be accomplished by tracing loan proceeds to the bank deposits, and tracing authorization for borrowing from the minutes of the board to the loan ledgers. In addition, a computer analysis can do the following:

1. Compare addresses of interest payees.
2. Match borrowings with repayments.
3. Check the schedule of late repayments.
4. Check the schedule of authorization of loan proceeds.
5. Check the list of loan recipients.
6. Check the list of addresses where loan proceeds were delivered.

5.6.5 Prevention

Proper documentation of loan documents, journal entries, interest coupons and stock certificates can aid in prevention of capital acquisition and repayment frauds.

Proper approvals include receiving approval of the board of directors for: borrowing, paying dividends and refinancing debt. Physical safeguards include keeping stock certificates and loan documents under lock and key. Also, conduct independent checks on the transfer agent and registrar.

Segregation of duties is also important in prevention. The authorization to borrow should be separate from handling cash and accounting. Authorizations to issue stock should be separated from the handling of cash; and accounting should be separated from handling cash, and dividends and interest.

5.7 CASH MISAPPROPRIATION

Although not a cycle, cash is the focal point of most entities. All other cycles flow through the cash account. Because there are so many different ways to misappropriate cash, this section covers cash exclusively.

Most organizations can divide their cash into two major categories: petty cash and demand deposits. Petty cash consists of cash on hand that is accounted for separately. It is reimbursed periodically, and the expenditures are then booked to the various accounts. Demand deposits consist of checking accounts maintained by the entity; savings or interest bearing accounts; and certificates of deposit and all other liquid investments that can be easily converted to cash.

5.7.1 Perpetration

Frauds perpetrated on the cash accounts are normally committed in conjunction with other cycles. The most common are the theft of petty cash and the theft of bank deposits.

Theft of Petty Cash

Petty cash thieves usually forge or prepare fictitious vouchers for reimbursement from petty cash. As an alternative, perpetrators frequently *borrow* from the petty cash account and fraudulently represent that the petty cash account is intact.

For example, the head security officer had custody of petty cash. He had altered legitimate receipts—primarily for postage—to reflect higher amounts. Postage is an overhead item that was loosely monitored. At a surprise count of the fund, only about $700 in currency and receipts were on hand of the $4,000 fund. Polygraph examinations were given to all security officers, but the head officer resigned before his test. A promissory note for the approximately $3,300 shortfall was executed by the former head officer. He had been with the company for seven years. The company estimated the loss at $12,000 but was unable to prove that this amount had been stolen.

Theft of Bank Deposits

Many times employees steal cash receipts prepared for deposit. In some instances, they change the amount reflected on the deposit. In other cases, they make no attempt to conceal the theft.

In one case, an employee of a food services business received daily receipts from sales along with the cash register tapes from two or three cashiers. The employee mutilated the tapes so they could not be read, then prepared the transmittal of funds for the comptroller, but kept the difference between the amount transmitted and the amount submitted to her by the cashiers. She sent the mutilated tapes to the comptroller with the deposit. The comptroller's office did not compare the deposit with the cash register tapes. The fraud was detected when one of the cashiers noted that the transmittal to the comptroller was small for a comparatively busy day. When questioned about tracing the transmittal amount to the cash register tapes, the perpetrator was unable to show completed tapes. The employee, who had been with the company two-and-a-half years, was fired but not prosecuted.

Employees, officers, and even outsiders can steal checks, both blank and signed. One case involved an employee—a grandmother—who was the sole bookkeeper for an electrical supply company in Omaha, Nebraska. She wrote the company's checks and reconciled the bank account. Over a period of five years she stole checks totaling $416,000, which she spent on herself and her family. In the cash receipts journal, she coded the checks as inventory; in fact, however, she wrote the checks to herself using her own name. When the checks were returned with the bank statements, she would simply destroy them. She confessed after she had a nervous breakdown, caused by continuous guilt from stealing, which she knew was wrong.

5.7.2 Detection and Prevention

Because cash can be counted exactly, most detection methods involving cash relate to its timely counting. The proof of cash is a standard audit technique that compares cash in the bank to reported cash on hand. Properly done, the proof of cash can not only account for theft, but also show overstatements or understatements by expense classification.

Timely and regular bank reconciliations by a person not responsible for handling cash will frequently reveal discrepancies. Good reconciliation methods include examining endorsements and dates, and if staff and time permit, referencing the checks to invoices, orders, and other relevant documentation.

For example, a misappropriation of funds was detected through a reconciliation of bank deposits with a collection log, which was normally kept by the accounting clerk, who at the time of the reconciliation was absent on sick leave. Because the accounting clerk prepared the collection log, the daily cash report, and the bank deposits, she was able to alter individual accounts receivable records and misappropriate almost $24,000. She accomplished this by preparing daily cash reports that reflected fewer cash receipts collected than were actually received, and depositing the lesser amount in the company's bank account. The accounting clerk processed virtually the entire accounting transaction. After the discovery of missing funds, she was fired, prosecuted, pleaded guilty, and was sentenced to ten years' probation. She had been with the company three-and-a-half years.

Auditors frequently use cutoff bank statements to ensure that expenses and income are reported in the proper period. Surprise cash counts sometime turn up situations of employees *borrowing* or floating small loans. It is critical that these counts be done on an irregular basis.

Cash thefts are sometimes reported by customers who have either paid money on an account and have not received credit, or in some instances when they notice they have not been given a receipt for a purchase.

As an example, a client of a branch of a large bank complained that there had been a $9,900 forged savings withdrawal from her account. The client indicated that she had recently made a $9,900 deposit at the branch and suspected that the teller who accepted the deposit may have been involved. The employee was interviewed and admitted to forging and negotiating the savings withdrawal. The teller had obtained the client's mother's maiden name and birthplace, fabricated a duplicate savings receipt book, and on an unscheduled work day went to the domiciling branch and posed as the client. The employee did not have any identification, yet was persistent enough to obtain an approval on the savings withdrawal.

Computer analysis of the following categories can sometimes turn up fraud in a cash account: checks that are missing, checks payable to employees, checks that are void, comparisons of deposit dates to receivables, and listings of cash advances.

It is absolutely imperative to implement tight control of cash and to maintain the duties of accounting, authorization, and custody.

In one case a fraud occurred at one of several campus cashier's offices maintained by a university for collecting and processing student tuition bills and other related charges. The perpetrator was employed as a teller for approximately five years before being promoted to head cashier. This position required reconciling daily cash register receipts to the cash transmittal and bank deposits, as well as preparing deposits for funds received from outside departments, such as the bookstore or dining service operations. These deposits involved substantial amounts of cash. As head cashier, the employee also prepared the initial accounting documents that served as the input to the various general ledger accounts, including accounts receivable.

The perpetrator's extensive knowledge and experience, coupled with the employer's trust, resulted in diminishing supervision, particularly of the cash register reconciliations. As a result, the perpetrator was able to manipulate the documentation and the control procedures necessary to conceal the continued embezzlement of funds. The employee, who had six-and-a-half years' service, was fired and prosecuted for stealing an estimated $66,000.

External Fraud for Personal Gain

CHAPTER 6:

External Fraud for Personal Gain

CHAPTER 6:

External Fraud for Personal Gain

6.1 Fraud Perpetrated by Outsiders

Fraud is not merely the product of internal thieves acting against their employers. Fraud in the accounting records may originate with outside suppliers and service providers as well.

It is not possible to determine the number of persons and bogus business operators engaged in crimes of this nature. Suffice it to say that the problem is extensive. By some estimates, nearly everyone at one time or another has been either a direct victim of such a crime, or an indirect victim through higher fees or income taxes.

6.1.1 Classification of Internal and External Fraud

As introduced in chapter 1, for the purposes of this Handbook, commercial fraud can generally be classified into two categories:

1. Internal fraud—that is, fraud committed against an organization by its employees, officers, or directors
2. External fraud—that is, fraud committed against an organization by arms-length parties (either individuals or corporations) who are outside the organization

Noncommercial fraud and other forms of white-collar crime also exist in which the fraudster is unrelated or external to the victim (an individual).

The Impact of Collusion

Some forms of external fraud can also be committed with the help of an internal fraudster—someone internal to the organization who is willing to assist the external fraudster commit his or her crime. Generally, internal personnel would need some form of an incentive—often in the form of a secret commission, kickback, or bribe—in order to be induced to assist in this manner.

Fraud involving parties both internal and external to an organization are sometimes referred to as *collusive frauds*. Another form of collusive fraud involves fraud committed by a group of people within an organization. Both kinds of collusive frauds exist because most internal controls are based on the principle of segregation of duties—this is circumvented by collusion.

Another form of collusive fraud, committed totally externally, is price fixing. When competitors agree to raise, fix, or otherwise maintain the price at which their products or services are sold, it is price fixing. The victimized customer of the colluders usually is not aware of the price fixing unless there is a whistle blower. And, as markets are served by fewer and fewer entities resulting from mergers, price fixing will probably become a bigger problem.

6.1.2 Reasons for Classification

Without some form of classification, the numerous kinds of fraud would overwhelm and confuse the *student* of this topic. Learning is enhanced when long lists are grouped and classified—for instance, students of a foreign language don't start at *a* in the English translation dictionary. Instead they start by studying the common elements of verb conjugation, pronouns, nouns and adjectives so that they can grasp a wider cross section of the language, and then put it all together when they begin to speak it. Of course, languages have many exceptions to the rules. Similarly, most foreign-language pocket guides present phrases by topic. For instance, phrases relating to money are separate from phrases relating to restaurants, travel, shopping and health; however, certain phrases could be applicable to more than one situation.

Much the same way, this Handbook's approach to grouping and classifying fraud enhances the CPA's ability to learn about the numerous kinds of fraud. As a result, you should have a greater appreciation for the wide variety of fraud that can occur, and should be better equipped to recognize the signs of fraud at first sight. However, some frauds are difficult to classify, fall into more than one category, or don't exactly fit into any of the established categories. These instances are mentioned as appropriate within the body of this Handbook.

6.1.3 Classification of Fraud in this Handbook

In chapter 5, we discussed a restricted group of frauds—those committed against an organization by its employees, officers or directors—otherwise known as internal fraud.

External frauds cover all remaining forms of fraud and represent a wide variety of frauds. This chapter covers those external frauds that can be classified by perpetrator. These frauds include:

1. Fraud committed primarily by individuals against a company, government, or other individuals; this is referred to as *external fraud for personal gain.*
2. Fraud committed primarily by a company against another company, government, or individuals; this is referred to as *commercial crime.*

Note that individuals using a corporate veil could also conduct certain of the frauds presented in this chapter. Similarly, chapter 7, which primarily covers fraud by corporations, includes fraud that could be conducted by individuals directly.

6.2 INDIVIDUALS VERSUS INDIVIDUALS AND CORPORATIONS

Individuals can commit many kinds of fraud against other individuals and corporations. Most of the victims of the crimes described in this section are generally manufacturers, retailers, wholesalers, service companies or other individuals; however, in some instances, victims can also include governments, financial institutions, and insurance companies.

6.2.1 Lawyers' Schemes

Overbilling for Time

Lawyers can easily commit fraud, largely because of the nebulous nature of the services provided. As one commentator indicated: the law lends itself to confidence scams. Contrasted to a plumber, for example, whose failure to make the contracted repair is quickly noticed, a lawyer's performance of an agreed to service is not always discernable. It

(Text continued on page 5)

could be merely some advice, a brief phone call or any number of innocuous, commonplace actions.

The victims of overbilling can include the lawyer's clients who are unable to assess whether the time billed by the lawyer is reasonable, and can also include government funded legal aid programs whose organizers are unable to assess whether the services billed were actually performed. When in doubt, a lawyer's invoices can be vetted; that is, they can be assessed by another lawyer for reasonableness regarding whether the services billed needed to be performed, and whether the time taken to perform the services was excessive or not.

Misappropriation of Trust Funds

Lawyers have access to funds provided to them by clients *in trust* to complete transactions. There are many cases of lawyers *borrowing* client funds because they are in personal financial difficulty. The most common crime associated with lawyers' trust funds is the misappropriation of client funds held in trust and the use of the money for the lawyer's personal purposes (for example, to subsidize a business, pay gambling debts, or support a life-style).

There are three kinds of misappropriation:

1. *Single transaction*: Client funds can be traced to an unauthorized disbursement (one-shot).
2. *Several transactions*: All trust-account activity is analyzed to determine which clients funds were used for unauthorized disbursements (lapping).
3. *Trust-account chaos*: Usually, this kind of misappropriation is caused by poor record keeping. Actual misappropriation of funds may or may not be found. Is the chaos the result of poor bookkeeping practices? Are there reasons for the failure to account (such as bad health, bankruptcy, intent to defraud, or loss of control due to numerous misappropriations)? The answers to these questions may emerge after a complete analysis of the trust account's activity has been made. According to the ethical rules of most states, if not all states, any use by an attorney of funds held in a trust account other than that for which the funds were placed in trust is considered a serious breach of professional conduct that may lead to disbarment, suspension or possible prosecution. There can never be a legitimate misappropriation of funds that an attorney holds in a trust account.

To uncover a case involving misappropriation of trust funds, the accountant should realize that lawyers regularly maintain two sets of bank accounts and related records, consisting of:

1. One or more bank accounts, books of account, and supporting documentation for the law practice itself.
2. A trust account together with any records reflecting the trust-account activity carried out on behalf of the lawyer's clientele. These are the most relevant records for investigating alleged misappropriation of trust funds. The primary documentation required for trust-account activity consists of bank statements and bank reconciliations for the trust bank account; the client's ledger, which outlines all receipts and disbursements made by the lawyer on behalf of the client concerning a particular transaction; and the client's file, which contains evidence of the transactions (for example, correspondence, the lawyer's

reporting letter, statement of receipts and disbursements, statement of adjustments, mortgage documents, out-of-pocket vouchers, and billings).

CPAs conducting an investigation of an attorney's trust account might also want to review the financial statements for the law practice. These records can be used to assess the successfulness of the lawyer's practice, and are most relevant when the lawyer is a sole practitioner.

See table 6.1, below, for an example of a misappropriation that would only be uncovered by a detailed investigation of the banking transactions conducted within a trust account.

TABLE 6.1 EVIDENCE OF A MISAPPROPRIATION OF A TRUST FUND.

January 1, 1991	Deposit of $30,000	Agrees with client file
January 5, 1991	Withdrawal of $10,000	Unauthorized by client
January 29, 1991	Deposit of $10,000	Unauthorized by client
January 31, 1991	Balance of $30,000	Agrees with client file

At the end of the month the trust liability to the client, as disclosed in the client file, is $30,000. However, $10,000 was temporarily removed during the month by an unauthorized transaction. Thus a misappropriation of the trust fund occurred.

Skip Towne, Esq. Case Study

After twenty years in practice, a lawyer, Skip Towne, Esq., had built up a large client base, including friends, business people and fellow church-goers. Mr. Smith, who was selling his home, retained Mr. Towne's services. At the time the transaction closed on August 3, 1998, Mr. Towne received $176,574 from the purchaser's attorney for deposit into the Skip Towne, Esq. trust account. Mr. Towne disbursed $5,000 of the funds in his trust account to cover various closing adjustments including outstanding utilities and tax bills. Mr. Towne also distributed $21,176 to his own account to cover the legal fees and other disbursements related to the closing. The balance ($150,398) due to Mr. Smith, as shown in the Closing Statement, was apparently paid in two distinct disbursements to Mr. Smith: an initial amount of $65,000 on August 10, 1998, with the balance of $85,398 on October 13, 1998. This final payment to Mr. Smith was, however, financed by the deposit into the trust account of funds that Mr. Towne received from new clients and other nefarious acts.

The specific funds in question, that is, $85,398 on hand as of August 10, 1998—were not paid to the benefit of Mr. Smith. Between August 10, 1998, and October 13, 1998, Mr. Towne made a payment of $80,000 to himself that he used to invest in his own real estate venture, and a payment of $5,398 to his other clients, to replace trust funds that had already been spent on unauthorized disbursements. To keep the ball rolling, Mr. Towne had to misappropriate funds from a number of other clients in order to repay Mr. Smith, in addition to producing false mortgage documents, forging signatures, and resorting to other acts of deceit.

Ultimately, Mr. Towne cleared out his trust account, abandoned his law practice, and disappeared, leaving behind at least eighty-five clients who had been defrauded. He has not been heard from since.

6.2.2 Directory Advertising Schemes

Perpetrators of directory advertising schemes usually target businesses. In this scheme the fraudster sells advertising in a nonexistent magazine or directory, and absconds with the proceeds. Many directory advertising schemes are perpetrated out of storefront operations. A fake (or in some instances, real) directory is presented to the potential victim. The victim contracts for the display or classified advertising, which will appear some months hence. By that time, the fraudster has collected the funds and disappeared.

6.2.3 Property Improvement Schemes

Fly-by-night operators, promising repairs to property at bargain rates, are a particular problem for elderly victims. The typical fraudster is a professional con artist who obtains business primarily from door-to-door solicitations. The tools of the trade are not hammers and saws, but bogus business cards and counterfeited or preprinted contracts involving the payment of up-front money. Note that these property improvement scams are a subset of procurement fraud, which is covered in more depth in chapter 7. Various forms of this scheme include substituting products, charging for false labor or overhead charges, and absconding with retainers and down payments.

Substituting Products

In a product substitution fraud, the fraudster typically promises a property owner a particular product or brand, and charges him or her for it but then substitutes an inferior brand without an appropriate price reduction. Thus the perpetrator reaps a windfall profit through this deception.

Charging for False Labor or Overhead

Many repair contracts call for labor, materials or overhead to be charged at cost, plus a specified contractor's profit as a percentage of that cost. Obviously the more the repairs cost, the more the contractor makes. By fraudulently inflating costs through the addition of bogus labor charges or overbilling of materials, the fraudster not only increases the profit but also can keep the difference between the actual and inflated costs.

Absconding With Retainers and Down Payments

The preferred method that seasoned professionals use is to simply negotiate money in advance, then disappear. This is essentially an advance fee swindle perpetrated specifically in the property-improvement or repair market. This method is advantageous to the perpetrator because it requires the least amount of capital: no storefront, props, or other accoutrements necessary—just "get the money and run."

6.2.4 Personal Improvement Schemes

The term *personal improvement fraud* covers the many schemes that prey on people's natural tendency to want to improve their job skills, appearance, education, or position in life. Fraudsters in this category primarily use mail order as an integral part of the scheme. Some common forms of personal improvement fraud are described below.

Vanity- and Song-Publishing Schemes

Vanity- and song-publishing schemes are common, and rely on the victim believing that he or she has talent in a particular area, such as art or song writing. These schemes are normally advertised in magazines or by direct mail. They usually offer to evaluate, for free, the victim's talent. Of course the victim is told after the evaluation that he or she is the newest undiscovered artistic genius. And for a hefty fee, the talent company will promote the artist's work. The artist then remits the fee, and the fraudster uses the funds for personal benefit, providing little or no services in the process.

Modeling Schools

Modeling schools appeal to the natural vanity of some people. Typically, the modeling school tells the student that he or she must have a portfolio of portraits to send to potential customers, ostensibly to enhance the victim's potential for getting modeling assignments. The victim is then charged greatly inflated prices for a photographer to take the pictures for the portfolio. Many modeling schools are not legitimate. They sometimes tout connections to famous people, or claim they have placed famous people, when in fact they have not. These schools get most of their business through mail order or newspaper advertising. Once a particular area is fleeced, the *school* pulls up stakes and moves on.

Diploma Mills

For a fee—usually a hefty one—a *diploma* can be granted to those persons who apply. The fraudsters usually claim the heavy fee is for *processing* the application or for verifying the experience necessary to acquire a degree. The hallmark of a diploma mill is the ease with which the *degree* is obtained, and the related cost. Victims usually apply for an advanced degree to enhance their career skills; however, diploma mills are not accredited, and their diplomas are therefore essentially worthless. Given the nature of this kind of business, there is usually some culpability on the part of the so-called *victim*.

Correspondence Schools

Legitimate correspondence schools offering advanced education do exist. However, there are also many correspondence schools with the same modus operandi as diploma mills, providing substandard education at superior prices. They are generally not accredited and offer little hope of job advancement.

6.2.5 Insider Trading Schemes

Insider trading involves the use of nonpublic information to make stock trades on a securities or commodities market. It could include purchasing shares prior to a good news release and can also include selling shares prior to a bad news release. The perpetrators of such crimes get rich, while other investors are unable to share in the wealth. Some might argue that this is a victimless crime, while others would say that the victims are the market as a group, because each and every trade is part of the market.

Criminal charges for insider trading have become the trademark of economic crime enforcement efforts during recent years. These efforts seek to encourage the confidence of investors in the fairness of the markets.

A surge of prosecutions for illegal insider information transactions began in the late 1980s when stock transactions were first subjected to sophisticated computer review, enabling investigators to identify unusual stock movements. Soon afterwards, when some meaningful piece of financial information about a company was released, investigators could quickly determine who had traded the stock heavily before the news release. If, for instance, a firm's president executed a transaction, it seemed likely, (though not assured), that he or she had acted on the information before it was publicly disseminated. The insider trading laws require that specified officers or directors of a corporation must report their trading activities. The fraudster, however, conveniently forgets to file the required information.

Of course, the notable cases of Ivan Boesky and Michael Milken remain the most infamous, and illustrate the staggering sums of money to be made from illegal stock trades. Boesky, the Wall Street arbitrage king, was sentenced to three years in prison and fined $100 million. In his plea agreement, he gave information that led to the indictments of so-called junk bond king Michael Milken, who eventually pled guilty to insider trading and was fined $600 million.

6.2.6 Homicide-for-Profit Schemes

Homicide cases are quite different from white-collar crime cases in that the perpetrator is a violent criminal, whereas most fraudsters are not violent. The tools of a murderer are guns, knives, ropes, water (for drowning), fire (for arson) and poison, whereas the tools of a fraudster are documents, books and records, computers, and calculators. The victim in a homicide case loses his or her life, whereas a fraud victim generally only loses some money.

But there is one main similarity, particularly when there is a financial motive for the homicide—the use of forensic accounting in homicide cases is similar to its use in fraud cases and may involve corporate- or personal-financial assessments, or both.

Generally, forensic accounting may be applied in homicide investigations for one or any combination of the following three purposes:

1. To analyze and determine a possible financial motive for murder.
2. To analyze financial documentation for possible investigative aids that may assist in proving murder.
3. To identify possible payments on a contract for murder.

Assessing Financial Motive

In determining a possible financial motive, the investigator must direct the accounting analysis primarily toward establishing and measuring any financial benefit to the accused as a result of that person's association with the murder victim. Benefit may be shown in any one or combination of the following methods:

- Payments by the victim to the accused (extortion).
- Assets such as real estate, collectibles, or antiques transferred to the accused.
- Insurance proceeds paid to the accused as a beneficiary under a policy.
- Other benefits, such as obtaining equity in a business or transferring of a partnership interest to the accused.
- Other motives that don't equate to a direct financial benefit, such as the imminent loss of assets, involvement in drug trafficking, or marital infidelity.

Accounting evidence is not generally as significant as viva voce evidence. It may, however, provide circumstantial evidence of a financial motive.

Assessing Financial Evidence to Assist in Other Ways in the Investigation

When assessing the financial matters of the victim in order to assist in a police investigation, the forensic accountant may seek to determine:

- The victim's business and social relationships and the identity of people with whom he or she had dealings.
- The existence of any debts owed either by or to the victim, and whether evidence exists to suggest the victim or debtor was resisting payment on them.
- The possibility of eliminating financial matters as a direction in which to pursue in the investigation.

Investigators should examine business and personal financial records, as well as financial-related evidence from the local real estate deed-mortgage recording office, lawyers, the will of the deceased, and insurance policies.

Robert Kilbride Case Study

On March 29, 1998, Mary Kilbride, wife of Robert Kilbride, a veteran police officer, was found dead outside her condominium complex. She had fallen from the twentieth floor balcony of their condominium. Eight days later, Robert Kilbride flew to the South Pacific to join Ms. Cathy Smith, whom he later married in May 1999 in Europe.

Ms. Sleuth, a forensic CPA, was called in to assist with the investigation. The police suspected Mary's death was not an accident—there was a $275,000 life insurance policy on her life that was paid to Robert Kilbride in late September 1998.

By way of background, Ms. Sleuth was told that in July 1997, Kilbride resigned his position from the police force. Friends and acquaintances said that about this time it was evident that Robert and Mary Kilbride were having marital problems.

Ms. Sleuth then worked with the investigating officer to determine all she could about the Kilbrides' life-style. The primary objective of Ms. Sleuth's accounting assistance was to summarize Robert Kilbride's financial activity for a period of approximately one-and-a-half years prior to Mary Kilbride's death, because of the allegation that Robert had murdered his wife Mary for the insurance proceeds. No summary books and records were available, a not uncommon situation in investigations of personal finances. Therefore, Ms. Sleuth had to reconstruct the financial facts before they could be interpreted.

The volume of financial documents was considerable. Kilbride had numerous credit cards, bank accounts and brokerage accounts in the United States, Canada and Europe. Kilbride was also involved in numerous business deals of varying nature and purpose.

In order to prove Kilbride's financial affairs, Ms. Sleuth completed the following:

1. A summary of Kilbride's financial history.
2. An analysis of Kilbride's estimated net worth as of the end of July 1997 and September 1998, based on bank statements, brokerage statements, correspondence, contracts, appraisals, loan applications and other financial documentation.
3. A source and application of funds analysis of Kilbride's financial activity from March 1997 to December 1998, primarily based on Kilbride's banking documents, credit card statements and brokerage statements.
4. A report on Kilbride's monthly deficiency based on the information in the source and application of funds analysis.
5. Graphs showing the cumulative deficiency from just prior to Mary's death to late September 1998, when the insurance proceeds were received.

These analyses revealed the following, which the investigating officer corroborated by viva voce evidence from former coworkers, friends, neighbors and other people who knew the Kilbrides.

1. When he left the force, Kilbride had no known source of steady income.
2. The Kilbrides' combined annual salaries were less than $60,000, yet they lived in an expensive condominium and had a leased luxury sports car.
3. After leaving the force, Kilbride's net worth declined considerably. He began to borrow heavily and sell off certain assets, including a rental property. He was also involved with various unsuccessful business ventures.
4. By March 1998, substantially all of Kilbride's net worth was represented by assets he owned jointly with his wife. These assets included the equity in their condominium, furniture, furs, jewelry and household effects.
5. Between the time of Mary's death in March and his receiving the life insurance proceeds in September, Kilbride spent more than $100,000 traveling throughout the United States, Canada and Europe. Although Kilbride had no known employment income, he and Ms. Smith rented a villa on the Mediterranean coast. He had approximately $15,000 in other income during this period. Kilbride financed his life-style primarily by selling more assets, obtaining further loans and making heavy use of credit cards.
6. In late September 1998, Kilbride received the $275,000 in life insurance proceeds from Mary's death.
7. Also in September 1998, Kilbride sold the luxury condominium; he and Ms. Smith continued to live in the Mediterranean villa until he returned to the United States in January 1999, when he was arrested.

In summary, the accounting evidence revealed that Kilbride enjoyed a life-style he could not afford. He was living well beyond his means—his expenses so greatly exceeded his income during the months before and after Mary's death that he would have been virtually bankrupt if he had not received the insurance money on Mary's life.

This evidence was very useful in establishing a motive for murder, and weighed heavily at Kilbride's murder trial at which he was found guilty.

6.3 INDIVIDUALS VERSUS THE GOVERNMENT

Fraud against the government is a general term for several kinds of schemes perpetrated against federal, state, and local governments or government agencies. Typically, frauds against the government committed by individuals involve one of the following: income tax fraud and benefit-program fraud. (See chapter 7 for a discussion of frauds against the government committed by corporations.)

6.3.1 Income Tax Fraud

According to some estimates, most taxpayers do one of the following:

1. Fail to disclose all their income
2. Take deductions to which they are not entitled

The most common income tax frauds involve categories of individuals who receive their compensation in cash. These categories include waiters, restaurant owners, bartenders, and bellhops.

For the Internal Revenue Service (IRS) to be successful with a claim for income tax fraud, intent must be proven—it is perfectly legal for taxpayers to manage their affairs to minimize their taxes—it is illegal for them to do so in a deceitful manner.

6.3.2 Benefit-Program Fraud

Another major category of fraud against the government generally involves making false statements of various kinds in order to obtain funds. The United States and other countries with strong social assistance programs are easy targets for fraudsters. The specific programs targeted include:

- Welfare benefits
- Medicare and Medicaid benefits
- Unemployment benefits
- Disability programs
- Student loan programs
- Housing programs

Often, rings of fraudsters apply for government benefits, resulting in very high losses to the government, and ultimately to the taxpayer through increased taxes.

According to a January 2001 report, the U.S. government has taken an increasingly active role in pursuing health care fraudsters. The rate of criminal convictions quadrupled from 1992 to 1999. At the same time, recoveries from civil fraud cases increased by more than 50 percent, and of the $1.5 billion the government recovered from fraud cases, $840 million was from health care cases, both public and private.

6.4 INDIVIDUALS VERSUS FINANCIAL INSTITUTIONS

Fraud committed externally against a financial institution can take many forms and can be committed by anyone who deals with such organizations, including individuals and corporations. The most common offenses committed by individuals—and sometimes corporations—are credit fraud, loan fraud, false mortgage security, real estate fraud, money transfer fraud, money laundering, and check fraud. These and other frauds against financial institutions, committed by individuals, are described below.

6.4.1 Financial Institutions and Fraud

Definition of a Financial Institution

For the purposes of this Handbook, a *financial institution* is any organization, whether domestic or international, that is engaged in receiving, collecting, transferring, paying, lending, investing, dealing, exchanging, and servicing money and claims to money. This also includes safe deposit facilities, custodianships, agencies and trusteeships.

Under the broadest concept, the term financial institution may be applied to institutions, such as cooperatives, export-import banks, investment bankers and mortgage bankers.

Legal Aspects of Bank Fraud

In most jurisdictions, financial institutions are insured by an agency of the government and are governed by related criminal statutes. For example, in the United States the broadest of all federal statutes is Title 18, U.S. Code, Section 1344. It covers all assets owned or controlled by a bank, as well as employees and outsiders. It prohibits any action that would defraud the financial institution, such as embezzlement, misapplication, false statements and related fraudulent behavior.

6.4.2 Credit-Card Fraud

Generally, credit-card fraud can be divided into two categories. In some instances, the fraudster uses credit information from one individual to obtain credit for use by another. For example, John R. Fraud, with bad credit, obtains the credit information of John Q. Smith, and applies for a credit card under the name of John Q. Smith, using John R. Fraud's address. John R. Fraud then makes charges on the account. When John Q. Smith protests, the credit-card company attempts to locate the real user of the credit card, John R. Fraud, who has since absconded.

The other common credit-card fraud involves duplicating credit cards and then using them to purchase high-value merchandise, for instance, jewels, furs, and other items that can easily be resold before the credit-card company catches up with the fraudster.

More attention should be paid to credit-card fraud because it is growing in volume and taking on international aspects. No longer is credit-card fraud local; the Internet has opened the door to global possibilities. A merchant extending credit on an Internet transaction has to rely on the honesty of the purchaser and the limited comfort a bank authorization provides. All too often, the merchant is stuck for the shipped merchandise and no payment.

6.4.3 Loan Fraud

Borrowers sometimes provide false information to a lending institution in order to obtain funds to continue business activity, or simply to fraudulently get money that they have no intention of repaying. Some of the most common schemes include loans to nonexistent borrowers, false applications with false credit information, bribery of a loan officer, borrower misapplication of funds, and single family housing loan fraud.

Loans to Nonexistent Borrowers

In a loan-to-a-nonexistent-borrower fraud, the borrower uses a false identity to obtain a loan. This scheme can be carried out individually by the borrower, or with the assistance of an insider, such as a loan officer.

Fraud committed by individuals can be difficult to detect, particularly if the identity documents of the fraudster match his or her details as provided on the loan application. Warning signs include:

- The borrower is unknown to bank personnel.
- No public credit report is available.
- The borrower or loan officer requests unusual loan terms.
- Loan application information does not check out.
- The proposed security has an inflated value.
- The proposed inventory (security) has an unrealistic value.
- There is no CPA associated with the financial statements.
- The loan officer's bonus is based on volume of loans funded.
- The proposed collateral is located outside the bank's market area.
- The loan proceeds are distributed prior to the loan's closing.

False Applications with False Credit Information

False information on the credit application can include overstated assets, nonexistent assets, understated or omitted liabilities, inflated revenue and understated expenses. For example, a borrower with marginal net worth might inflate the asset and income figures on his or her personal financial statements to convince the loan officer of his or her credit worthiness. The loan officer and others involved in the bank loan approval process can often detect these schemes by observing one or more of the following:

- Appraisals-valuations that defy common sense and local knowledge
- Appraisers who are paid on basis of appraisal amount
- Large loans beyond experience and expertise of the loan officer
- Borrowers who default on the first payment

- Numerous payment extensions, or payments that are placed on nonaccrual status
- No audit trail for verifying application information
- Applicant reports receiving loans from many other banks

Bribery of Loan Officers

Statutes (for example, Title 18, U.S. Code, Section 201) prohibit any officer, director, employee, agent or attorney of a bank from knowingly soliciting or receiving things of value in connection with bank transactions. In the usual scheme, a borrower offers an officer an inducement to grant a loan that would not otherwise be made (for instance, because the borrower has little or no credit, or because the borrower is not using his or her real name).

(Text continued on page 15)

Senior loan officers can often detect these schemes by observing one or more of the following:

- The life-style of the originating loan officer is beyond the means provided by normal compensation.
- The loan officer has unreasonably high productivity.
- The loan officer's compensation is based on volume productivity.
- Loan agreements contain terms unreasonably favorable to the borrower.
- There is a pattern of disbursements to particular agents, brokers, appraisers, finders, and so on.
- There are multiple loans to the same borrower with the same agents involved.
- The loan or other bank officer has a financial interest in the customer's project, or stockholdings in a bank subsidiary profiting from the business.

Borrower Misapplication of Funds

Borrower misapplication is most common when the borrower has little or no personal risk in the collateral, for example, real estate. The highest risk real estate loans are those in which the lender provides all the funding on a nonrecourse basis. The most common ways borrowers misapply loan funds are as follows:

- Kickbacks or profit interests in construction activities
- Brokerage or real estate fees
- Property management fees
- Related-party vendors
- Closing-statement prorations of rent, taxes, and other items
- Land flips
- Sale of property rights, such as laundry or cable TV
- Misappropriation of operating proceeds or loan proceeds
- Misappropriation of escrow payments

Single Family Housing Loan Fraud

One variation of the misapplication-of-funds fraud is the borrower who purchases single family housing units, ostensibly for personal use, but in reality as rental property or in some instances for resale. When applying to a financial institution, the fraudster usually misrepresents his or her ability to finance the property and make payments. Usually loan officers uncover these frauds by observing one or more of the following:

- There is an unrealistic change in commuting distance.
- A high-income borrower has little or no personal property.
- New housing expense is 150 percent or more of the previous expense.
- Bank deposits are listed in round amounts on application.
- The borrower reports overlapping dates of current and prior employment.
- The previous employer is listed as out of business.
- A high-income borrower does not use a professional tax preparer.

- The appraisal shows a tenant as the contact person on an owner-occupied house.
- The initial title report shows delinquent taxes.

6.4.4 Real Estate Fraud

Real estate fraud is essentially a specialized form of loan fraud committed either by individuals or corporations. Financial institutions, especially the savings and loan associations in the United States, were badly hit in the 1980s due to fraud committed in the real estate area. These schemes are often perpetrated in concert with the insiders of financial institutions.

Land Flips

A land flip is the practice of buying and selling a parcel of land very quickly, often in a single day or month, at a successively higher price to related parties, until a lender—who believes the transaction is at arm's length—provides financing on an unrealistically inflated loan amount. The key components of the scheme in sequential order are as follows:

1. The same piece of property is sold back and forth between a borrower—the fraudster—and dummy or shell corporations.
2. Each time the land is sold, the price is inflated.
3. To support each sale, the borrower secures an appraisal based on an unrealistic or favorable set of assumptions, or performed by a friendly, incompetent or dishonest appraiser.
4. The borrower goes to a financial institution—the victim—and mortgages the property for its *appraised* value, keeping the grossly inflated loan proceeds.
5. The fraudster defaults on the loan.

False Appraisals

Fraud perpetrators use false and inflated appraisals to support loans larger than the true value of the property. Appraisers are either parties to the fraud or paid off, or they are merely unqualified—that is, easily fooled by bogus transactions like land flips—to perform the appraisal.

Nominee Loans

Nominee loans are those made in the name of a *straw* (dummy) borrower or agent—that is, a borrower having no substance—while the identity of the real borrower is undisclosed to the lender.

Double Pledging Collateral

This scheme involves fraudulently pledging the same collateral with different lenders, before the related liens are recorded and registered. This obviously hinders the lender's ability to look to the collateral as a source of recovery when the borrower defaults.

Real Estate Fraud Detection

Lenders or other interested parties can often detect real estate fraud by observing one or more of the following warning signs:

- A single borrower has received multiple loans.
- The same appraiser has appraised two or more different properties for the same borrower within a short period of time.
- The same appraiser has made successive appraisals of the same property at high values in a short period of time.
- The property was bought or sold many times in a short period.
- The borrower is a *shell* with no real substance or a holding company whose substance lies hidden in its numerous subsidiaries.
- The buyer is obviously shopping for a loan instead of a long-term banking relationship.
- The seller of the property is another bank.
- The borrower has a prior default history.
- The borrower has a history of loan payoffs by obtaining other, larger loans.
- The loan application contains requests for several loans to different persons on the same property.
- The borrower requires the loan as a condition before delivering large deposits to the bank, with the loan being the inducement for establishing a continuing banking relationship.

6.4.5 Money Transfer Fraud

Wires totaling two to three times a bank's assets may be processed every business day. It is rare that wires do not at least equal a bank's total assets, and they can sometimes be ten times the assets for banks that have a large correspondent network. The process is highly automated at most banks.

In the most common money transfer fraud, an outsider or bank employee with access to the correct identification numbers needed to wire transfer funds, steals the funds. In one case in Chicago, a bank insider with knowledge of the wire transfer codes and procedures conspired with his friends to wire nearly $70 million out of the country. The scheme was detected (early enough to avoid a loss to the bank) when the transfer was made from a customer's account, thereby overdrawing the account balance.

Warning signs for this kind of fraud include:

- Clerks rather than more senior personnel perform actual processing.
- Managerial personnel conduct frequent overrides of the established approval authority controls.
- There is evidence of wires to and from offshore banks in countries known for their bank secrecy laws.
- There are routine high volume, high dollar transfers.
- There are frequent wires for persons with no account at the bank.
- Access to the wire room is often not properly restricted.
- Employees become very comfortable with the routine of the job and with their coworkers.

Variations of these schemes involve misrepresenting the customer's identity. The fraudster will use pretext telephone calls to obtain correct account information from the bank. Then the fraudster obtains the codes from an insider. Thereafter, the fraudster makes a telephone call to transfer the funds out of the bank.

6.4.6 Money Laundering

Money laundering refers to the process of turning *dirty* money into *clean* money. The primary objective is to conceal the existence, source or use of illicit money and thus the underlying offence—whether the offence is trade in illegal narcotics, robbery, fraud, illegal political contributions, tax evasion, prostitution or any other criminal activity. Money launderers may also want to obstruct investigative efforts, preserve assets from forfeiture, and evade taxes.

Perpetrators may launder money in the country in which the crime is committed or where the funds originated; more often, however, they send the money across an international border. Usually they deposit the money in a bank or other institution in a tax haven and it comes back *clean* in the form of salaries, loans, fees or services.

Money Laundering Methods

There are three main methods for laundering money:

1. Through legitimate *fronts*
2. Through couriers and smurfs
3. Through the cooperation of a bank insider who ignores the reporting guidelines

Each of these methods has certain unique characteristics; however, they also have some common characteristics:

1. Large cash shipments
2. Large volume of wire transfers to and from offshore banks (However, not all offshore wire transfers involve money laundering—see below.)

Legitimate Fronts. Many money launderers open a legitimate front business that handles a great deal of cash—for instance, a casino, restaurant, parking lot, vending machine company, or pawnshop—and then deposit the ill-gotten gain along with the legitimate income of the business. Perpetrators then commingle the illegal cash with the legitimate receipts thereby disguising any illegal sources. They then withdraw the *cleaned* money or wire-transfer it to a final destination.

Interested parties, for example a bank or bonding company, can usually detect this kind of fraud by observing one or more of the following warning signs:

- Accounts accumulate deposits that are subsequently transferred out.
- Cash deposits from sources are not identified as customers of the business.
- There is a sudden and unexplained increase in the volume of cash deposits.

Money launderers can use gambling casinos. The ill-gotten cash is used to purchase chips. Later the launderers exchange the chips remaining at the end of a controlled (carefully limiting losses) gambling session for money and receive the proceeds in the form of a check from the casino, thereby creating a seemingly legitimate paper trail.

Smurfing. One variation of the money laundering scheme is to use special couriers, called *smurfs*, to make relatively small deposits and withdrawals. For example, cash deposits of $10,000 or more must be reported to the Internal Revenue Service (IRS) on a special form called a Currency Transaction Report (CTR). To avoid this reporting requirement, smurfs make deposits or withdrawals just below this threshold amount.

Banks and other interested parties can usually detect this kind of fraud by observing one or more of the following warning signs:

- Withdrawals made in numerous transactions just under $10,000.
- Customers who are not account holders exchanging large amounts of small bills for large denomination bills.
- Inquiries as to policies of the bank regarding reporting currency transactions.
- Large dollar volume of cashier's checks and money orders sold for cash to customers who are not account holders.
- Persons shown as unemployed and self-employed on a CTR.

Breaches of the Reporting Guidelines. In still another variation, the money launderer conspires with a bank insider, who agrees to make deposits for the money launderer and forego the reporting mechanisms. The bank gets free use of the deposited funds, and in some instances, the bank officer is compromised through a bribe or kickback. Banks can usually detect this kind of fraud by observing one or more of the following warning signs:

- An account with many different individuals making deposits, and only a few making large withdrawals.
- Accounts with accumulated deposits that are subsequently transferred out.
- High dollar limits and large numbers of bank customers exempted from CTR requirements.
- An incorrect or incomplete CTR.

Money Laundering Mechanics

Although laundering and offshore banking conjure up images of financial wizardry and international tax lawyers and accountants, most illegal activity involves the simple addition of some layers to the basics common to ordinary business transactions. In essence, laundering works like this.

Party A, who has come by the dirty money (or legitimate money that needs to be laundered) gives it to Party B, who is the laundryman. Party B sends the money offshore where it is deposited and funds are subsequently disbursed or laundered and then returned to Party A for use.

During the laundering, Party B, having received the money from Party A, sets about concealing it. Having the money in currency upon receipt makes the job easier. If the money is in paper (checks, and so on), Party B may have to first start the laundering process by converting it to local currency. Party B has, or sets up, one or more local companies, of which he or she is the owner, manager or employee, depending on the relationship to Party A.

Now the offshore part of the process begins. Party B goes to a tax haven lawyer and establishes an offshore company: loan companies, finance companies, or trusts are preferable. Party B's name does not appear anywhere in the legal documents.

The company in the tax haven opens an offshore bank account. Party B travels to the haven with the currency, and Party B or the lawyer buys a cashier's check at the bank with the tax haven company as remitter. The lawyer then draws up the necessary loan documents to show a loan from the haven company to Party B's local company. Party B then returns home with the cashier's check. Thus, the money is brought back home as a loan (which being capital, not revenue, is not taxable) and is *clean*.

Party A on his own, or through Party B, now makes use of the laundered funds by drawing out salaries, obtaining loans from Party B's local company, paying dividends, opening a corporate expense account, using a company car, and so on.

Party B's local company files appropriate tax returns and makes note of payments, or at least interest payments. Interest is deducted on the company's tax return. If the company loses money, it has a tax offset. Party B does nothing illegal in the local country and, of course, makes interest payments on the loan payable to the offshore company, allowing further funds to be moved.

If a law enforcement agency questions the loans, the company will obtain full documentation from Party B's attorney in the tax haven. Inquiries beyond documents will be blocked by the haven's secrecy requirements.

Offshore Banks and Tax Havens

There are many reasons, some legitimate and some not, why money launderers transfer money and other valuable securities from one jurisdiction to another jurisdiction that has secret banking privileges. These foreign jurisdictions are commonly referred to as tax havens because, in addition to bank secrecy laws, they had no income taxes so people or companies first used them to (legally) minimize or to (illegally) evade taxes.

Tax haven is now a misnomer, since funds may be deposited for reasons other than escaping tax. Tax havens have grown in popularity in recent times as one of the few means of placing funds beyond the reach of creditors or other investigators. It did not take long for criminal organizations and individuals to exploit the sanctuary of the tax haven. With the development of multinational banking systems and international business and commerce, it became easy to put together sophisticated laundering schemes to move the proceeds of crime to foreign banks protected from intrusion by law enforcement officials.

The World's Tax Havens. Switzerland has a long history as an international tax haven, imposing little financial regulation and strict secrecy laws. Many other countries have jumped aboard the bandwagon. The key tax havens include—

- Bermuda and the Caribbean: Antigua, Bahamas, Caymans, Montserrat, Netherlands Antilles, St. Vincent, and Turks and Caicos.
- Central America: Panama and Costa Rica.
- Channel Islands: Guernsey and Jersey.
- Pacific: Hong Kong, Singapore, and Vanuatu.
- Other locations: Liberia, Bahrain, Liechtenstein, Switzerland, and Cyprus.

Offshore Facilities. Typically, the tax haven's biggest domestic industries are banks, financial institutions, companies, trusts, agents, accountants and attorneys who collectively constitute offshore facilities. Facilities that are available in tax havens include—

- *Banks.* There are two classes of banks. Class A banks conduct local business transactions in the tax haven. Class B banks exist on paper only, as they conduct no local business transactions.
- *Companies and trusts.* Companies can be incorporated in the tax haven; trusts (such as family, estate, or other kinds) can be set up.
- *Offshore agents, accountants and attorneys.* These are an essential element of the offshore facilities in a tax haven.

The Tax Haven's Rationale. Tax havens encourage offshore facilities for economic, political and social reasons, all of which benefit their residents. For example, offshore facilities generate up to 20 percent of the Caymans' revenues, balance the budget in Montserrat (through licensing fees) and have a huge impact on local economies, particularly those of economically emerging countries.

For example, in 1964 the Caymans had one or two multinational banks and virtually no companies. By 1981 they had thirty multinational banks, 300 Class B banks, and about 13,600 companies, the latter handled by a small number of lawyers, accountants and agents. The Caymans' total population in 1981 was about 15,000.

Many havens claim that the United States blames them for problems that it is unable to solve domestically. Furthermore, offshore competition is so stiff that it is estimated that if one country were to cease being a tax haven three more would start. (When Switzerland relaxed its secrecy laws, Bahamian and Caymanian business grew at a rapid rate.) Also, bank brokers move from island to island as laws tighten or loosen.

A local Bahamian bank executive summed it up when he said

> The Bahamas must do things which are not allowed in the United States because to do things which are allowed in the United States is noncompetitive, since in every instance the United States does it better than the Bahamas do. The Bahamas are therefore compelled in banking and trust operations to appeal to unallowable activities and by inference to appeal to activities disallowed in the United States.

Secrecy. The vital characteristic of a tax haven is that it allows offshore facilities to conduct their affairs behind a veil of secrecy. Tax havens offer not only secret, numbered bank accounts but also corporate laws and secrecy provisions that prevent law enforcement officials from intruding. In addition, lawyers from tax havens offer a further level of secrecy because they too are shielded by the haven's secrecy laws, they maintain attorney-client privilege, they sometimes do not know who their clients are, or they may be coconspirators, or any combination thereof.

Tax havens view secrecy as a necessity for keeping offshore business. Business people from various parts of the world (the Middle East and South America, for example) consider secrecy to be a normal characteristic of business affairs. Flight capital (money being sent out of politically unstable countries) has to be transferred secretly. Thus, it is not only criminals but also politicians and governments to whom secrecy is attractive.

Civil secrecy exists in common law as the result of a British case, *Union* v. *Tournier* (1907). This case established that a banker had a duty to treat his customer's affairs as confidential. Many havens follow this law. Some jurisdictions have passed stringent, criminal laws to buttress *Tournier*—for example, the Bahamas and the Caymans. Corporate laws in the havens also aid secrecy by permitting nominee owners and bearer shares, prohibiting disclosure of the beneficial owner, not requiring financial statements and audits, and allowing the purchase of companies off the shelf.

Quite apart from the law, secrecy prevails in some tax havens by virtue of inadequate records, unskilled administrators and corruption.

Vehicles Used to Transfer Funds to Tax Havens. Individuals or businesses can use several kinds of institutions to transfer funds to tax havens. These include banks with international branches or facilities, smaller trust companies and banking institutions, shipping companies, real estate companies, travel agencies, money changers, insurance companies, finance companies, brokerage and investment companies, international trading companies, holding companies, and multinational corporations. The transfers themselves may be legal or illegal. The transfer can be accomplished by means of letters of credit to a bank in a tax haven, a bank draft, a wire transfer, or the transport of cash itself.

File Folders. Money launderers can purchase a set of legal papers in tax havens—for example, legal documents, financial statements, and banking documents dated some years before they are purchased. These documents make it appear that the company has been in business for several years. In reality, of course, it never previously existed. These companies have no substance.

Tax Havens and Law Enforcement. The combination of offshore corporate entities and secret bank accounts in tax havens permits entities to construct a maze of financial transactions. The tracing of assets becomes a very complex task. The transferring of questionable funds from one tax haven jurisdiction to another greatly compounds the complexity.

Enforcement problems are pervasive, affecting not only criminal but also civil actions (such as divorces, bankruptcies, and so on). Investigating cases takes a tremendous effort, and conviction is by no means certain. There is no central clearing house to handle offshore inquiries.

Investigations into Narcotics Trafficking

Narcotics trafficking is currently the primary source of laundered funds. The sophistication and complexity of laundering schemes are virtually infinite and are limited only by the creativity and expertise of the criminal entrepreneurs who devise the schemes. Organized crime uses banks and other financial institutions in the course of laundering as routinely, if not as frequently, as legitimate businesses use banks for legitimate purposes.

Previously, much of the investigation into narcotics trafficking occurred on the street in which the drugs were followed to identify the dealers. Although this led to many successful prosecutions, it seldom exposed the leaders of the organizations. The problem with a street investigation is that the authorities generally cannot make a buy from, or a sale to, the top person in the organization without the use of an informant, who is generally unreliable. Furthermore, because the sentences received by drug traffickers were often so light, perpetrators considered the risk worth taking—and the leaders of the organizations continued to be insulated.

Currently, law enforcement authorities obtain financial documentation during seizures in order to establish that certain individuals possess goods that far exceed their known sources of income. This technique has made possible the successful prosecution of the leaders in drug trafficking schemes. Generally investigators use two methods to prove the flow of funds obtained from narcotics trafficking:

1. Net worth analyses
2. Sources and uses of funds

6.4.7 Check Fraud

Check fraud is a general term for the attempted negotiation of bad checks at a financial institution. Typically con artists prey on banks in an attempt to negotiate fraudulent or fictitious instruments. Common kinds of check fraud include forged, altered, and stolen checks; new account fraud; and check kiting.

Forged, Altered, and Stolen Checks

Most attempts to defraud banks involve one or more of the following:

1. Checks bearing the forged names of makers, endorsers or payees.
2. Altered checks showing increased amounts.
3. Counterfeit checks.
4. Stolen checks passed by others.

Bank officers and other investigators can detect this kind of fraud by observing one or more of the following warning signs:

- Obvious written alterations on checks
- Illegible maker, endorser or officer signatures
- Checks imprinted with a maximum amount, or the term *void*, or *nonnegotiable*
- Unprofessional printing
- Business checks presented for cash instead of deposit

New Account Fraud

Check fraud is much more likely to occur in new accounts than in established accounts. Bank employees must make special efforts to properly identify the potential new customer, without offending existing customers. Banks should establish screening criteria that must be enforced by everyone handling new accounts. These employees must take prompt, decisive action to manage or close (or both) apparent problem accounts.

Most perpetrators of new account fraud use false identification. Examples include fraudulent birth certificates, fraudulent passports, duplicate social security numbers, fraudulent voter registration cards, stolen credit cards, stolen driver's licenses, stolen paychecks, front (shell) businesses, fraudulent student-identification cards, and disguised identities (including post office box mail address, lock box rental, mail forwarding, telephone answering service, and rented office space).

New-account criminals are professionals. They use false identification to open new accounts and steal money before the bank collects the funds. Bank officers can normally detect new-account fraud by observing one or more of the following warning signs:

1. The customer resides outside the bank's normal trade area.
2. The customer rushes to open an account and obtain a loan.
3. The customer's dress or actions, or both, are inappropriate for his or her stated age, occupation or income level.

To help prevent this kind of fraud, banks should consider adopting the following procedures:

1. Implement well-defined procedures for increasing employee awareness of new-account fraud.
2. Establish specific guidance about acceptable identification and its reporting.
3. Require detailed verification of customer's information, including—
   —Previous checking account history (internal and external investigation).
   —Credit reports and credit scoring systems.
   —Dun & Bradstreet reports.
   —Better Business Bureau reports.
   —Special requests for no mail contact.
   —Post office box or hotel address.

Check Kiting

Check kiting is a term for building up large apparent balances in one or more bank accounts, based on uncollected or floated checks drawn against similar accounts in other banks. As banks decrease the amount of time taken to clear checks, this kind of fraud is becoming less common. Although many individuals engage to some degree in kiting, a commercial customer can perpetrate this scheme by using several bank accounts to increase available cash reserves.

The brokerage firm, E.F. Hutton, committed one of the most significant check-kiting schemes perpetrated in the United States. They engaged in a $20-million kiting scheme to decrease the cost of their funds during the late 1980s. The resultant bad publicity eventually led to the company's demise.

Check Kiting, Illustrated. In commercial bank accounts established over a period of time to avoid suspicion, a fraudster starts with little or no money in Bank A and Bank B, and writes $5,000 in checks on each for deposit in the other:

	Bank A	**Bank B**	**Total**
Apparent Balances	$5,000	$5,000	$10,000
Actual Balances	-0-	-0-	-0-

The process is quickly repeated (for example, the next day) with $8,000 in deposited checks:

	Bank A	**Bank B**	**Total**
Apparent Balances	$13,000	$13,000	$26,000
Actual Balances	-0-	-0-	-0-

A $6,000 down payment is made on a Mercedes from a check written from Bank A.

	Bank A	**Bank B**	**Total**
Apparent Balances	$7,000	$13,000	$20,000
Actual Balances	($6,000)	-0-	($6,000)

The next day additional checks for $4,000 each are written and deposited into each account:

	Bank A	**Bank B**	**Total**
Apparent Balances	$11,000	$17,000	$28,000
Actual Balances	($6,000)	-0-	($6,000)

The balances are then paid to a travel agent, and the fraudster takes a long trip:

	Bank A	**Bank B**	**Total**
Apparent Balances	-0-	-0-	-0-
Actual Balances	($17,000)	($17,000)	($34,000)

Check Kiting Characteristics. Bank personnel usually uncover check-kiting schemes by observing one or more of the following warning signs:

- Frequent deposits and checks in same amounts.
- Frequent deposits and checks in round amounts.

- Frequent deposits of checks written on the same paying bank, which is not the deposit bank.
- Little time lag between deposits and withdrawals.
- Frequent Automatic Teller Machine (ATM) account balance inquiries.
- Many large deposits made on Thursday or Friday to take advantage of the weekend.
- Large periodic balances in individual accounts with no apparent business explanation.
- Low average balance compared to high level of deposits.
- Many checks made payable to other banks.
- Bank willingness to pay against uncollected funds (note that not all payments against uncollected funds are check kites, but all check kites require payments against uncollected funds).
- Cash withdrawals with deposit checks drawn on another bank.
- Checks drawn on foreign banks with lax banking laws and regulations.

Slowing the Bank-Clearing Process. Before the days of sophisticated computer systems, a check-kiting scheme could develop using less paper, fewer financial institutions, and smaller amounts than are commonly used toay. Banks can still be hit with large losses when a fraudster slows down the bank clearing process. Typical fraudsters' procedures include—

- Using counter checks without any computer or Magnetic Ink Character Recognition (MICR) coding.
- Providing insufficient information on checks (for example, using an incomplete name of a bank and branch, leaving out the account number, giving an illegible signature).
- Making errors on the face of checks such as date and figures.
- Defacing the check (for example, by using staples).
- Placing stop payments on certain documents.
- Having accounts in institutions other than chartered banks (that is, trust companies and credit unions).

New Techniques. It is now very difficult to effect a check-kiting scheme employing the same procedures as in the past. Banks are reluctant to accept counter checks; more significantly, checks usually take only one day to clear. This is true even for checks issued on out-of-town or out-of-state banks. The financial institutions claim that, in the near future, checks will clear instantaneously. To counteract the tightening of bank procedures, the fraudster has had to increase the number of financial institutions used, the dollar amounts, and frequency of checks issued.

Check-Kiting Scheme Investigations. The main issues to be addressed when investigating a check-kiting scheme are as follows:

1. The loss does not necessarily occur at the time of detection. Banks are usually put at increasing financial risk over a period of time.
2. Accounting evidence must show that—
   a. Control was exerted over a number of accounts.
   b. A loss did occur.

c. Economic risk has increased as shown by day-by-day analysis.
d. Every time the perpetrator withdraws money from the system of accounts (in excess of the deposits put into the system), the bank incurs a loss or risk of loss.
e. The volume of inter-account checks is high.

3. The bank must determine whether it gave implied credit to the accused through *daylight overdraft* privileges, which allow an overdraft balance at the end of a business day to be cleared up before the close of the next business day to cover the previous day's overdraft.
4. The timing of the investigation and the availability of legible microfilm documentation are important.
5. Documentation of the *modus operandi* needs liberal use of visual aids.

Accounting Assistance. When investigating check-kiting, the CPA should—

- Identify the fraudster-controlled accounts because the financial institutions where they are maintained risk suffering economic losses.
- Identify and demonstrate the loss. This task is difficult because there is a mistaken tendency to regard loss as occurring at the termination of the check-kiting scheme. In fact, however, the risk of loss usually builds up day by day, over a period of several months. Recognition of the economic loss occurs when the perpetrator abandons the fraudulent activity for whatever reasons (this is equivalent to the game of musical chairs—the loss isn't recognized until the music stops).
- Perform a day-by-day analysis to show both the buildup of the loss and the increase in economic risk to the financial institutions.
- Recognize that a check-kiting scheme could take place over an extended period of time without the knowledge of the bank. This is an issue that is frequently raised in court. This component is an educational aspect for many: lawyers, police, bank officials, laymen, and even CPAs find check kiting difficult to understand.
- Try to accomplish the difficult task of demonstrating to a court of law that this case was not merely an unbroken circle of checks and that this *shell game*, which was apparently tolerated by the financial institutions, resulted in economic loss to them.

Mr. I.M. Kiter Case Study

Recently, between January and the middle of March, an extremely busy, well-respected professional, Mr. I.M. Kiter, operated a massive check-kiting scheme that employed at least eight bank accounts at three separate financial institutions. For two-and-a-half months he was able to falsely inflate the value of his accounts by issuing checks to or from his various accounts.

About four weeks before the scheme was uncovered, one of the financial institutions was sufficiently concerned about the statuts of Mr. Kiter's accounts that it would only accept certified checks for deposit. This had the effect of reducing the clearing time to zero days or in certain instances to minus one day (the check was certified the day before it was deposited). Despite these restrictions, Mr. I.M. Kiter was able to continue his check-kiting scheme for the following reasons:

1. The other financial institutions did not require deposited checks to be certified.
2. Some overdraft privileges were permitted.
3. Mr. Kiter spoke with the financial institutions daily and explained away his suspicious conduct.
4. Checks were not return marked *not sufficient funds* (NSF), as required by bank policy, because the bank's normal policies were changed for Mr. Kiter, a *good* customer.
5. The bank permitted daily daylight overdraft privileges.

Forensic accountants performed an analysis of the deposit and disbursement activity in the various bank accounts. With the exception of the closing bank overdraft, the deposits totaled about $87.5 million, of which more than $85 million represented money circulated among the eight accounts controlled by Mr. Kiter. The total amount of actual deposits from noncontrolled accounts only amounted to about $2.5 million. The ending balance in one of Mr. Kiter's accounts at Anytown Bank was a negative $1.7 million. This overdraft balance resulted in a loss that was fully absorbed by Anytown Bank. Forensic accountants also performed an analysis of an account maintained by Mr. Kiter at Bigtown Bank for the period March 1 to March 10. This analysis indicated that Bigtown Bank permitted ongoing overdraft privileges to Mr. Kiter in amounts up to almost $1 million. Closer inspection revealed the extent of Mr. Kiter's abuse of the daylight overdraft privileges.

This practice was confirmed by the review of Bigtown Bank's credit correspondence, and demonstrated that the departure from Bigtown Bank's policy allowed Mr. Kiter to continue the check-kiting scheme in an uninterrupted fashion. In fact, when the kiting scheme fell apart, it provided Mr. Kiter with a defensible position for court purposes (that is, his conduct was condoned or *blessed* by Bigtown Bank).

The practices of Bigtown Bank also raised the questions as to whether the economic loss suffered by Anytown Bank was because of the check-kiting scheme, or because of the conduct of Bigtown Bank. Evidence introduced during the trial did not establish that the banks were aware of the kiting scheme. However, there was evidence that Bigtown Bank knew that Mr. Kiter was having some cash flow difficulties pertaining to closing a number of real estate deals. Handwritten comments from the Bigtown Bank branch manager to his credit department indicated that—

1. The bank closely monitored Mr. Kiter's account.
2. The bank allowed certified checks to cover the overdraft daily.
3. The bank tolerated daily overdraft amounts of approximately $ 1 million.
4. The bank received substantial revenues via overdraft and service charges (an example of the bank greed factor).
5. The bank indicated at a meeting held with Mr. Kiter on February 25th that it would permit the overdraft arrangement to continue for another sixty days.

6. Mr. Kiter had social connections and was a source of business for the bank.

Although Mr. Kiter was found guilty, the judge's ruling implied that prior knowledge of the check-kiting scheme on the part of one of the banks weakened the prosecution's case.

6.5 Individuals versus Insurance Companies

Insurance fraud generally consists of a presentation to an insurance company of a materially false or misleading written statement relating to either an application or claim for insurance. Fraud occurs not only when there is an actual loss (that is, a claim is made based on bogus information), but also when there is a risk of loss. This distinction is important for insurance fraud because insurance policies relate to risks. Accordingly, if an insurance policy based on a material misstatement is placed, the insurance company is the victim of a fraud because there was the risk of a claim, even if no claims are made on the policy.

Some insurance policies relate to risks faced by individuals, whereas others relate to risks faced by corporations. This section deals with both kinds.

Computers have become an important tool in discovering insurance fraud. The most common use is to let the computer discover clusters or interrelated data; for example, an unusual number of claims filed from the same address. This kind of screening is effective in insurance scams because the fraudsters often work in consort, for example, with doctors or auto repair shops, to file inflated claims that a search engine seeking commonality can discover.

6.5.1 Life Insurance Fraud

Life insurance is a policy that pays the insured's beneficiary a predetermined amount of money in the event of the insured's death. Common life insurance frauds include homicide fraud, staged-death fraud, preexisting health condition fraud, and double-indemnity fraud.

Homicide Fraud

A beneficiary of a life insurance policy may commit homicide to collect benefits. In these cases, there are actually two victims—the person who has been murdered (see section 6.2.6), and the insurance company, which is required to make a payment on the policy.

Staged Death Fraud

An insured might fake his or her death in order to collect benefits. A variation of this scheme occurs when a policy is taken out on an insured who is already dead.

Preexisting Health Condition Fraud

An otherwise uninsurable person obtains a life insurance policy through false health statements on the application describing preexisting health conditions. The normal, minimal medical examination would not be sufficient to expose the condition. The insured hopes to die of causes unrelated to the *feared* condition—that is, a condition that would otherwise prevent the policy from being issued—and without an autopsy being performed, so that the insurer will pay the policy benefits.

Double Indemnity

In some cases, a beneficiary of a life insurance policy will report the death as having been accidental in order to obtain twice the face value of the policy. A variation of this scheme occurs when a beneficiary attempts to make a suicide appear to have been accidental.

6.5.2 Casualty Insurance Fraud

Casualty insurance covers the personal injuries and property damage that result from an accident or other covered occurrence. While accidents can occur anywhere and at any time, a large number of casualty claims involve injuries sustained in traffic accidents. The following are the common casualty insurance frauds:

- Staged accidents
- Mortgage insurance fraud
- Legitimate accidents with false claims
- Personal injury insurance fraud
- Fraudulent claims

Staged Accidents

A staged accident is one in which, for example, an individual will purposely pull out into the path of an oncoming vehicle or will allow themselves to be rear-ended in order to cause a collision. A fraudulent claim is then made for nonexistent personal injuries or a falsely inflated claim is made for real injury. These kinds of insurance fraud usually involve *rings* of individuals, including unscrupulous doctors, attorneys and claim adjusters.

Mortgage Insurance Fraud

Mortgage insurance is a policy that guarantees mortgage payments to the lender if the purchaser of the property defaults on those payments because of death or disability. A typical mortgage insurance fraud is a variation on a staged accident fraud—for example, an employee who is laid off from work claims that he is disabled, so his mortgage is paid via his mortgage insurance policy.

Legitimate Accidents with False Claims

In many cases, an individual is involved in a legitimate accident and later exaggerates his or her personal injuries (usually soft-tissue injuries) to bilk the insurance company.

Personal Injury Insurance Fraud

Personal injury insurance fraud usually involves lying about the circumstances of the cause of an injury so as to bring it within the insurance coverage. For example, a worker covered by workers compensation insurance injures his back while working at home but reports it as a job-related injury to come within the workers compensation insurance coverage.

Fraudulent Claims

A fraudulent claim is one in which, for example, an insured's auto is brought into a body shop for repair after a legitimate accident. The body shop inflates the claim, typically to cover the deductible. The body shop may then pay a cash bribe to the claims adjuster or intentionally cause additional damage to the car to maximize its profit.

In another example, an insured seeks the cooperation of a scrap yard that has the capability to crush autos. The insured has his auto crushed and files a theft claim. If the auto is not recovered within a reasonable span of time, the claim is paid. The insured then pays the scrap yard for destroying the vehicle without a trace.

In still another variation, a wrecked vehicle is located and insured. A bogus accident is concocted and a fraudulent claim is filed. Using the same vehicle, this scheme is often repeated with different insurance companies.

6.5.3 Health Insurance Fraud

Health insurance is a policy that covers someone's health in the event that the person is injured or becomes ill. Common health insurance schemes include mobile labs, bundling and unbundling claims, and collusion between an insured and a provider.

An insurance industry representative reported, in January 2001, that fraud claims in both the public and private sector reach about $53.9 billion annually. The U.S. government has increased the funding of law enforcement agencies in the health-care fraud area, with some U.S. attorneys offices setting up special health-care fraud units. According to one U.S. attorney, health-care fraud is the most active area of white-collar crime, which includes going after clinical labs and individual doctors, among others.

A growing fraud related to credit-card fraud is debit-card fraud. Many banks are now issuing a combination ATM/debit card/credit card rather than three separate pieces of plastic. Although merchants, generally, cannot check whether there are funds in the bank supporting a debit card purchase, they can check a credit card with a phone call. No doubt as the problem grows, protective steps will be installed to stop the fraudsters. Until the preventive measures catch up, prosecuting and publicizing the fraud will help slow the growth of this new threat.

Mobile Labs

In the usual mobile lab scam, a group of people set up a *lab* in a storefront located in a blue-collar, low income area, often where English is the second language. They then pass out fliers in the parking lot of a minimum wage manufacturing firm, offering *free* physicals to people who have medical insurance. After filling out a family history, the insured is subjected to extensive tests for a variety of maladies, and the average physical ends up costing the insurer three to four thousands dollars. When the insured returns for the results of the tests, the lab is gone.

Bundling and Unbundling Claims

Bundling and unbundling claims is the practice of physicians or clinics billing separately for medical services performed at the same time. For example, an insured woman has a hysterectomy performed and at the same time she also has her appendix removed. The physician, however, bills the insurance company as if the appendectomy was a completely separate procedure.

Insured-Provider Collusion

In collusion between an insured and a provider, the provider furnishes the insured with a bill for services not actually rendered. The insured makes an application for reimbursement to the insurance company, and the proceeds are divided between the insured and the provider.

6.5.4 Property Insurance Fraud

Property insurance is a policy that covers an individual or corporation's property from loss (whether stolen or destroyed), up to a predetermined amount of money. Common property insurance schemes include: staged false theft, repossessed household goods, pawned personal property, and arson.

Staged False Theft

In staged false theft, an insured secretes property he or she owns and reports it stolen, or alternatively reports property stolen that he or she never owned.

In a recent case involving Michael Jackson CDs, a music distributor had misjudged the demand for the CD and had excess inventory on hand. A theft was then staged in order to offload the excess stock, which was then destroyed. When forensic accountants revealed the lack of demand and the excess inventory, the distributor dropped his claim.

Repossessed Household Goods

Repossessed household goods fraud occurs when, for example, household items (furniture, appliances, and so on) are repossessed, and the insured reports the property was stolen.

Pawned Personal Property

When pawning personal property, a fraudster may inflate the value of his or her personal belongings, insure them, and then pawn them for a lesser amount of cash. The fraudster then reports them stolen and files a claim. Once the insurance payment is received, the fraudster then redeems the items from the pawnshop with a portion of the insurance payment, and pockets the difference. These schemes can be risky to the perpetrator, however, because in most states pawnshops are required to check customer identification and keep records of their transactions, in order to facilitate police investigations of reported thefts.

Arson

Arson is the purposeful destruction of property by fires, sometimes for profit. For example, an insured may be about to lose his or her house, car, or business due to an inability to make loan payments. The insured sets fire to the property to collect the insurance proceeds. Alternatively, an insured may replace an item with something less expensive when he or she remodels after the fire.

Arson can also be committed by companies, which then file claims under their property insurance policies as well as their business interruption policies. This is covered in chapter 7.

CHAPTER 7:

Commercial Crime

CHAPTER 7:

Commercial Crime

7.1 OVERVIEW

7.1.1 Definitions

The terms *white-collar crime, economic crime,* and *commercial crime* are not legal ones and are often used interchangeably. This chapter covers the distinctions between these terms.

White-Collar and Economic Crimes

Although scholars differ widely in their definition of white-collar crime, the *Dictionary of Criminal Justice Data Terminology,* published by the U.S. Bureau of Justice Statistics, defines white-collar crime as: "non-violent crime for financial gain committed by means of deception by persons whose occupational status is entrepreneurial, professional or semi-professional and utilizing their special occupational skills and opportunities; also non-violent crime for financial gain utilizing deception and committed by anyone having special technical and professional knowledge of business and government, irrespective of the person's occupation." This definition includes most if not all of the crimes and behaviors described in this Handbook.

Economic crime has a similar definition regarding its objective and methodology, that is, crime committed for economic gain by means of deception; however, economic crime is broader in its scope than white-collar crime: it could also include violent crimes committed by people without any particular occupational status—for example, armed robbery.

Commercial Crime

The term commercial crime is frequently used as a substitute for the terms white-collar crime and economic crime. However, for purposes of this Handbook, a more restrictive definition is adopted: that is, commercial crime is white-collar crime committed by an individual or a group of individuals in a company for the benefit of that company and, indirectly, themselves.

This distinction, that is, between fraud committed *against* a business or commercial entity, and commercial crime committed *by* a business or commercial entity—is a useful one. Historically, our legal system, institutions, and even the procedures adopted by auditors have tended to focus more on conventional fraud committed purely for personal gain. In recent years, however, awareness has been heightened to the possibility of the business or commercial entity itself being the perpetrator.

Frauds against investors and environmental crime are two examples that have received increasing media attention.

7.1.2 Victims of Commercial Crime

Victims of commercial crime can include—

- Customers—for example, through false advertising and price fixing.
- Competitors—for example, through industrial espionage and intentional copyright infringement.
- Creditors—for example, through a planned bankruptcy.
- Investors—for example, through false financial statements and other securities fraud.
- The general public—for example, through environmental abuse.

In addition, the practice of organizational bribe giving may victimize any one of the above groups—for example, the general public when a bribe is given in the awarding of a government contract.

7.1.3 Extent of Commercial Crime

Two decades ago commercial crime received much less media attention than today, largely being confined to a short paragraph or two in the business section of the nation's newspapers, if it was mentioned at all. Today's front-page stories are a testimony to the current widespread public interest in and concern about commercial crime. Scholars attribute this growing emphasis to, among other things, a greater skepticism about the behavior of persons in authority. The alleged crimes of Whitewater involving President Clinton and his associates only deepen the mood of distrust of those in prominent places.

Statistics suggest that there is some reason for distrust. For instance, KPMG Peat Marwick's 1998 Fraud Survey reported that false financial statements caused losses of $1 million or more in 42 percent of the reported instances, whereas in the 1994 survey, losses of this magnitude represented only 24 percent of the total losses.

While it is true that surveys only deal with reported crime, what is clear is that the extent and value of reported commercial crime is on the increase. Many experts believe that many frauds go unreported and that the extent of unreported commercial crime is also on the increase.

7.1.4 Responsibility for Commercial Crime

Some scholars debate whether individuals should be held responsible for crimes committed on behalf of their organizations. Although some direct benefit accrues to the perpetrator, far more benefit accrues to the organization.

Regardless of whether the organization is held liable, the frauds are a direct result of some human action or interaction: if a business is like a dynamite charge, someone must push the plunger.

Most criminal statutes require that the guilty person have the required criminal intent. However, an organization can be held liable even if it were unaware of or did not participate in the fraud. The law recognizes two theories of organizational responsibility:

1. *The identification theory.* The organization is held liable when the employees and organizations can be viewed as one and the same, for example, a small business owner who has incorporated.
2. *The imputation theory.* The organization is held responsible for the actions of its employees through the doctrine of *respondeat superiour,* a seventeenth century doctrine that means "let the superior respond." The legal theory was developed from civil lawsuits to prevent employers from denying financial responsibility for the acts of their employees.

7.1.5 Characteristics of Commercial Crime

While commercial crime can take many forms, often it is distinguished by one or more of these characteristics: tolerance, diffusion of harm, and rationalization.

Tolerance

While awareness of commercial crime has increased in recent years, there still remains a somewhat greater tolerance for this form of crime as compared to violent crimes such as armed robbery, or those involving drugs. This greater tolerance may stem not so much from the nature of the crime itself, but rather from the perception of the perpetrator as being somehow more *civilized.* Anybody with strength, decent aim, or access to poison, can commit murder, but only a limited number of *respectable* corporate executives or directors are in a position to violate antitrust legislation.

Diffusion of Harm

Another notable characteristic of most kinds of commercial crime is that there are often numerous victims who are frequently unaware that they have been harmed. Death from smog or asbestos poisoning is very likely to be slow and insidious, and its victims will be hard-pressed to relate their terminal illness to its precise cause, given the complicated nature of other possible contributing factors. A factory worker with cancer is not likely to be certain whether it was the toxic chemicals that he handled for fifteen years, the fact that he smoked too many cigarettes, or bad genes or bad luck that will shorten his life.

In many other cases of commercial crime, the harm tends to be widely diffused and, for each person, rather insignificant. But these can still be significant crimes. Companies can earn millions over the course of a year by charging higher prices for products that do not meet the standards they are alleged to attain. Few people who pay for a package of one-hundred thumb tacks will take the time and energy to count the contents of the package to be certain that they have gotten their money's worth; it would be an easy and safe venture to put ninety-two tacks in each package, and some merchandisers find the temptation irresistible. Similarly, a customer will most likely remain unaware that the gasoline pumps at a service station are calibrated so that they get fewer gallons than those for which they are charged. Even if they come to know about these kinds of issues, most customers would shrug them off as not worth the trouble it would take to do something to remedy the situation; at most, they might take their business elsewhere.

Rationalization

Perpetrators of white-collar crime are known for providing elaborate excuses for their crimes, and the nature of such explanations may be a major distinguishing mark between them and street offenders. It has been posited that embezzlers typically claim that they are only borrowing the money; they intended to repay it once they had covered the bills and other financial demands vexing them. Commercial criminals will similarly rationalize their behavior; for example, antitrust violators usually maintain that they are seeking to stabilize an out-of-control price situation when they conspire with others to fix prices, and they are likely to insist that power-hungry prosecutors and investigators are singling them out.

7.1.6 Investigation and Prosecution of Commercial Crime

The diffuse nature of most commercial crime poses a particular law enforcement dilemma. Without complaining witnesses, policing has to be proactive instead of reactive; that is, the enforcement officials themselves have to decide where the offenses are being committed and how to go about stopping them. Enforcers obviously cannot cope with all the violations and must decide on rules to guide their efforts. Should they go after the behaviors that cause the most harm? Should they take on the bigger offenders, or concentrate on the *smaller fry*, where their chances of success are much better? They can readily accumulate ten convictions in a year against ten insignificant companies, whereas it might take three years to win a victory over one huge corporation. Besides, the resources of the large organization might allow it to win its case, regardless of the lawless nature of its behavior.

7.1.7 Causes of Commercial Crime

Because businesses are bottom-line driven, it has been posited that they are inherently prone to committing crime, yet not necessarily criminal. Without necessarily meaning to, organizations inherently invite commercial crime as a means of obtaining goals. For example, a department manager's concern with reaching assigned goals, may lead the manager to maximize his or her department's own interests to the detriment of the organization, or to the detriment of society as a whole.

Organizations can also be criminogenic—prone to producing crime—because they encourage loyalty. Accordingly, this is because—

1. The organization tends to recruit and attract similar individuals.
2. Rewards are given out to those who display characteristics of *a team player.*
3. Long-term loyalty is encouraged through company retirement and benefits.
4. Loyalty is encouraged through social interaction such as company parties and social functions.
5. Frequent transfers and long working hours encourage isolation from other groups.
6. Specialized job skills may discourage company personnel from seeking employment elsewhere.

These reasons in turn cause company personnel to sometimes perceive that the organization might be worth committing crime for.

Another aspect that makes companies criminogenic is their compensation structures, particularly for corporate executives who are most likely to be the perpetrators of commercial crime. Compensation packages for senior personnel usually include a component based on the results of their company or department, either through stock options or bonuses. Typically, senior executives have a greater amount of compensation tied to results than do other employees. Because commercial crime is so diffuse, and the likelihood of being caught is low, senior executives may perceive that the incentives to "enhance the success of their organization" through commercial crime will outweigh the risks.

7.2 FORMS OF COMMERCIAL CRIME

Today, the realm of commercial crime can be said to primarily involve offenses against laws that regulate either one or both of the following: the marketplace or the established standards of conduct for professional and political life. Some of the most common forms of commercial crime are described in this section, along with Case Studies and other examples that illustrate the salient features of such crimes.

The first two cover *shams,* which Webster's Dictionary defines as ". . . an imitation or counterfeit purporting to be genuine [*noun*] . . . ." and "to act intentionally so as to give a false impression [*verb*]."[1] Shams are the result of the activities of a confidence trickster or con artist who has been able to obtain money from the public by various means. Generally, there are two kinds of shams: corporate shams and investor fraud.

Although these shams are discussed separately in this chapter (due to the size of each section), in many cases the perpetrator (the corporate con artist) and the victim (individuals) of the shams have similar characteristics, as does the way in which the sham is operated. However, they have two major distinctions:

1. In the corporate sham a corporation exists from which the pitch is made. This is in contrast to an unincorporated individual making a pitch, not on a corporation's behalf, but on his or her personal behalf.
2. In investor sham the nature of what is being *sold* to the victim differs. For example, an investor sham typically involves making a speculative investment, whereas a corporate sham typically involves the purchase of something tangible.

The remaining sections of this chapter include the following kinds of fraud as committed by companies: procurement fraud, industrial espionage, finance fraud, securities fraud, environmental abuse, economic extortion, health care fraud, and possession of property obtained by crime.

7.2.1 Corporate Shams

Corporate shams generally involve something counterfeit or false. In this case the corporate sales pitch appears to offer something genuine, yet there is no underlying substance. The perpetrator of the crime is often a con artist acting through a corporate entity. In fact, by using the *corporate veil* as a shield from the public, the con artist gains an appearance of

[1] *Merriam Webster's Collegiate Dictionary*, Tenth Edition, 1993.

respectability and substance that he or she would otherwise lack. The con artist's wares may consist of one or more of the following:

- Products oriented to individual consumers (as opposed to products that companies would buy) that are sold by false advertising.
- Franchises or distributorships that the victim purchases in order to run a business.
- Solicitation of money donations towards a charitable or religious cause.

Generally, shams that are carried on through an incorporated business involve pyramid sales schemes, mail order sales, advertising to be placed in charitable programs or flyers, or donations to charitable organizations. Newer forms of corporate shams that are becoming more common are the selling of franchises, and other get-rich-quick schemes, such as the selling of vending or arcade game machines: the purchasers then set up their own business using the franchise or the equipment bought.

When a con artist hides behind a corporate veil, some or all of the following characteristics may apply:

1. The con artist uses expensive letterhead, emblazoned with a worldly name and a classy address, to impress potential victims.
2. The company has a very informal corporate structure, and a very short life span.
3. The company's accounting systems are primitive or nonexistent.
4. The company conducts an extensive and appealing advertising campaign.
5. If a product is offered, the product itself may be of questionable value, and there is seldom, if any, post sale servicing.
6. The customer is expected to pay for the product via cash or readily negotiable checks on (or before) delivery.
7. Once received, the cash is quickly removed from the company through the payment of commission expenses, salaries, bonuses or management fees, so that the con artist can reap the immediate benefits of the scheme.

The key to the corporate sham, as with any sham, is the effectiveness and the speed with which the sales pitch brings results. The method of delivering the sales pitch may range from telephone solicitation (via a boiler room operation), to either cold calls, or advertising in local newspapers, or both.

Possible red flags for a corporate sham include elaborate representations that demonstrate the quality of the product, proposed earnings that are excessively high for the franchise, or an apparently hard-sell pitch to raise money for a purported charitable purpose.

Finally, you should be aware of the arguments put forward by defense counsel in corporate sham cases. Some of the issues defense counsel might raise include:

- *Caveat emptor*—let the buyer beware.
- Some of the money received was in fact directed to the promoted charitable purpose.
- The investor is at fault: that is, for not working hard enough at a franchise operation to make it succeed, or for not waiting long enough to receive the goods that would have eventually been shipped, and so on.

Merchandise Swindles or False Advertising

Merchandising frauds include all frauds perpetrated against purchasers of merchandise and services. If you have ever paid for an item and received something less than advertised, you have been the victim of a merchandising swindle or false advertising.

These frauds generally fall into one of the following four categories:

1. Representations that the purchase is a bargain when in fact it is not—for example, department stores raise the price of a product significantly one day and then the next day drop it back to where it had been, maintaining in their advertising that it now is *on sale.*
2. Collection of money for one product and substitution of another of lesser quality or cost—for example, claims have been made that shoes are alligator when in fact they were made of plastic.
3. Misrepresentations regarding the quality of the product—for example, a company selling glass *demonstrated* in television commercials that its car window product was so perfect that when you looked through it you could hardly believe there was anything between you and the outside scene; it was later proved that the ads were filmed from inside a car with the window rolled down.
4. Failure to deliver the product or service—for example, in bait and switch tactics, stores advertise a specific product at a strikingly low price, but then, when the customer tries to buy the item, it is no longer available. It is the customer's presence and attention they want to attract—once they have him or her listening, they assume that slick sales tactics can accomplish the rest of the deceit.

Defraud You in Writing Case Study

Between September 1997 and June 1998, Smith and Jones, partners of Defraud You in Writing Inc. committed fraud by obtaining funds from the public for goods they did not intend to supply.

Smith and Jones operated the business through telephone solicitation whereby books were offered for sale, and customers' names were entered into a drawing for a trip to the Caribbean via Acme Tours. Door-to-door sales people would follow up on the calls and try to obtain orders for the books. The orders set forth the terms, the method of payment, the time and method of delivery, and an announcement for a drawing on a certain date. The drawing date was inserted in a blank on the order form, the first draw being December 31, 1997.

From the evidence of Mr. Sleuth, forensic accountant, during the period between October 1997 and May 1998, the actual net cash receipts from orders by members of the public totaled $75,291 (after allowances for returned checks) on 1,867 orders.

Defraud You in Writing's suppliers were not paid during this period, so the total number of orders filled was 311. In fact, during the three months with the largest sales, (December, February and March) no books were ordered from Defraud You's suppliers. Instead, substantial effort was being made to increase the sales force (and thus the revenue), and new premises were being sought.

The judge in this case believed that Defraud You in Writing used the 311 orders to create a camouflage for the business' real activity: to obtain funds for orders they never intended to fulfill.

As for the drawing, no arrangements had been made with Acme Tours to enable the winner to take the trip.

Franchise and Distributorship Frauds

Both franchise and distributorship frauds are characterized by a *get-rich-quick* business opportunity that involves a large up-front purchase of equipment, supplies, and promotional materials. Many such schemes are part of a pyramid scam.

CookieVend & Run Inc. Case Study

CookieVend & Run Inc. was incorporated in March 1997 to sell cookie vending machines. CookieVend's headquarters were located in New York City. Its office staff generally consisted of the president, general office manager, secretary-treasurer, bookkeeper, and three typists.

Shortly after CookieVend's incorporation, a series of ads were placed in newspapers across the country. These ads offered a substantial guaranteed income, which could be earned for an investment of $3,000 to $9,000. Although the ads differed somewhat from paper to paper, they all offered a part-time job that could net the right person an income of $2,000 per month or more.

In addition to the office staff, CookieVend employed a sales staff of approximately ten people to interview the respondents to the ads. These sales reps traveled independently of each other and were provided with a corporate brochure and other material that instructed them on what to promise the new distributors.

Some 180 people purchased these distributorships for an investment of between $3,000 and $9,000 each, depending on the number of vending machines purchased. Supplies of cookies and insurance were also purchased. CookieVend's total sales from April to December 1997 were approximately $1.2 million.

In the ensuing year, not one distributor was successful in his or her business. The complaints were generally as follows:

1. The quality of the vending machines was very poor.
2. Three distributors never received their vending machines (twenty-three machines in all).
3. Cookies were stale when received by the distributor.
4. The price of cookies increased from fourteen cents to twenty cents each soon after the distributors purchased their machines.

5. The company did not honor claims of damage to machines in accordance with the insurance protection policy on the agreement.
6. The company did not honor its three-year repair warranty on vending machines.
7. The company did not attempt to address any reasonable complaints.

Evidence of Fraud. All of CookieVend's management personnel were found guilty of fraud and received jail sentences. The evidence that formed the basis for the case against them was as follows:

1. CookieVend's revenues and expenses showed that its level of profitability was directly attributable to the sale of machines. This also showed that the sale of cookies resulted in losses, thus CookieVend had a motive to sell machines rather than cookies.
2. CookieVend's primary disbursements were for commissions, advertising, travel, and business promotion. These expenditures occurred during a period when the distributors' complaints about product quality fell on deaf ears.
3. The profit-loss experience of the distributors was much worse than the profit-loss statements represented in the newspaper advertisements. One of the highest performing distributors realized a gross profit, assuming all cookies were sold, of $375, on an investment of $7,941 over a period of eighteen months.
4. CookieVend never purchased a liability policy although the distributors' purchase agreements represented that a policy did in fact exist.
5. The distributor agreement set out a nonrescission clause specifically stating, "The distributor is not relying on any oral or written expressions, promises or warranties made by anyone to consummate this transaction."

Charity and Religious Fraud

Jim Bakker, former head of the defunct PTL (Praise the Lord Club) has brought international attention to religious fraud. The essence of his scheme was to sell "lifetime partnerships" in a luxury hotel, which his followers could use for life. Prosecutors were able to show that Bakker's plan was completely unworkable, because many more partnerships were sold than could ever be accommodated. Bakker used the money to pay himself and his lieutenants millions of dollars in salaries and bonuses. He was convicted under federal mail fraud statutes.

Other kinds of charity and religious groups resort to fraud as a way of obtaining *contributions.* In the most common of the schemes, fraudsters operating in boiler rooms call unsuspecting victims and raise funds for allegedly good causes or for worthwhile organizations. The funds collected are not used for their intended purpose, or the fraudsters fail to disclose that they keep the majority of the funds raised for administration costs and give the sponsoring charity or religion only a small portion of the money collected.

Rob M. Blind Case Study

Between January 1997 and July 1998, Rob M. Blind and I. Swindle committed fraud by developing a scheme through the medium of telephone solicitations that induced the public to contribute funds allegedly for charitable purposes—to benefit the blind.

The operation, *Help the Sightless Associates,* carried on by Rob and his associates, was reasonably simple. They hired three or four blind musicians, who joined other sighted employees for a tour of several cities. In each city they planned to visit, they conducted a telephone solicitation campaign: literally by going through the yellow pages and calling every business listed. The firms solicited were asked to buy an ad in a program, which was to be distributed at a concert to be held in that city.

If the firm refused to advertise, it would be asked to buy tickets to the concert that it could use, give away, or allow to be given away on its behalf.

The *Help the Sightless Associates* was not a charitable organization and never applied for registration as such. There is no record of them donating anything to the blind other than paying the musicians who gave the concerts.

As for the dollar amount of the fraud, according to Mr. Sleuth, forensic accountant, the total gross receipts for 1997 and part of 1998 were $252,327. These funds were used in the following manner:

Payments to the blind musicians	–50 percent
Payments unaccounted for	–48 percent
Expenses	–2 percent
Total	100 percent

7.2.2 Investor Frauds

Like corporate shams, investor frauds use techniques designed to produce a quick return or benefit to the company that is the subject of the con. The techniques generally used are telephone solicitation, personal cold calls, or spreading the sales pitch by word of mouth among a particular group of individuals, such as doctors or dentists—who typically have high incomes or high net worth, or both, but possess limited financial or investment expertise. The con artist may succeed in persuading a member of the group to introduce him or her to other members, thus creating confidence in both the scheme and him- or herself. The investors are actively encouraged to spread the word to their close friends about this opportunity for an investment. These activities are often perpetrated through a pyramid or *Ponzi* scheme—both of which are described below.

The key to the con is generally a direct pitch to the investors' greed—that is, promises of high returns within a short period. The scheme may entail investment in precious metals or precious or semiprecious gems, and has been known to embrace items, such as antique coins and commodity futures. Investor frauds have even extended to what is commonly known as flips of real estate.

Although many of the characteristics of a corporate sham discussed in section 7.2.1 apply equally to investor frauds, there are two characteristics that are unique to investor frauds:

1. An extensive and appealing get-rich-quick advertising campaign is conducted, suggesting to the victims that easy money can be made with very little effort.
2. Investors, once the investment is determined to be a con, do not want any publicity that would expose the foolishness of their investment.

Chain Referral (Pyramid versus Ponzi) Schemes

Chain referral schemes are based on the same idea as the well-known chain letter. This is a particular kind of sham, which could involve products, or may involve only investments. In one example of a chain letter, the con artist starts the chain letter by sending a letter to five or more people requesting (on some pretext—often preying on people's superstitions) the recipients to mail money to the con artist. The letter also instructs each recipient to send the letter to a further five people with the request that money be sent to the names in the first two tiers of the pyramid. The third tier recipients in turn repeat the process of mailing the request for money and adding themselves to the bottom of the pyramid. Often there is an instruction that only four or five tiers should receive the money; the top name dropping out with the addition of a new name(s) at the bottom. By the time the chain reaches the seventh or eighth level (if the chain continues that long), the multiplier effect creates enormous wealth to those higher up in the chain, because they receive money from the geometrically growing lower tiers.

Of course, things other than money can be the objects of chain letters. Some involve recipes, Christmas cards, and other harmless items. However, chain letters don't work indefinitely. That is because someone in the lower level inevitably fails to mail out his or her five letters, and the chain is then broken; usually only those in the upper levels profit.

Chain referral schemes, also called pyramids or Ponzi Schemes (after the notorious Charles Ponzi who successfully employed the scheme in the early twentieth century), are based largely on the same principal. The difference is that some are legitimate and some are not. Pyramid sales structures are generally legitimate, and Ponzi schemes are usually illegitimate.

For example, many products sold exclusively in the home, such as Amway merchandise, can be legitimate forms of pyramids. Individuals are recruited to sell merchandise. They in turn recruit their friends and colleagues to sell, and get a cut of their commissions. This recruitment continues on down, with those in the upper levels receiving a portion of the commissions from several different layers of sales personnel. However, because of the turnover in sales personnel, most people fail to achieve a sufficient level in the chain or pyramid to make the touted commissions. They often get discouraged and quit, further depressing the chain.

Illegal pyramids (Ponzi Schemes) exist as well. One common variation is for a fraudster to place mail order ads promising wealth to individuals for performing work in their homes for services such as stuffing envelopes. When the victim responds to the ad, they are informed that the *opportunity* requires sending in money. In return, he or she receives a letter suggesting the victim place a similar ad and collect money in the same way, using the same letter. In other words, the fraudster is telling the victims in effect, "do the same thing to others that I just did to you."

Another typical Ponzi scheme involves the diversion of investment funds. This fraud words as follows: A company will open its doors as an investment firm, promising better than average returns on its investment. When the company receives money from investors A through G, the money is diverted to the personal benefit of the principals. When additional money is received from investors H through L, those funds are used to pay off investors A through G. When funds are received from investors M through Z, this money is used to pay off investors H through L, or at least to pay interest, and so on. The money paid out to the early investors, therefore, is not from returns achieved on investments, but rather a diversion of new investments. This pyramid continues until the scheme collapses.

Many operators simply set up a mail or telephone operation, collect funds, then close the operation and move, only to reestablish a similar operation and repeat the scheme. Law enforcement officials acknowledge a significant problem with chain referral schemes, but readily admit that they are incapable of adequately controlling the problem.

These schemes, or variations of them, cannot go on indefinitely because they require a constant stream of money to cover the diverted funds. When the flow of new investments fall below that level, there is insufficient cash to pay off old investors, and the scheme collapses. The chain referral schemes are not dependent on a particular product or service, but rather on the method of diverting funds. Common chain investment schemes include franchising, sales distributorships, investment and securities of various kinds, and merchandise.

Finally, it should be noted that many chain referral schemes involve small amounts of money that are taken from many victims. Because victims typically feel foolish about being fleeced, they frequently do not file charges. And even when complaints are made, the police do not give these crimes priority because of staffing and budgetary commitments. As a result, many chain referral operators stay around a long time.

7.2.3 Finance Fraud

False Mortgage Security

False mortgage security is a term used to refer to security that turns out to be nonexistent or to have a value far lower than was represented. This is a kind of loan fraud whereby the perpetrator is usually an individual acting through a sham corporation, and the victim could be a bank, but is more likely an individual or another corporation.

The usual characteristics of false mortgage security fraud are as follows:

- An investor is persuaded to make a loan or invest funds on the assurance that repayment of the loan or investment will be fully protected and secured in some way.

- When the touted investment fails to materialize, the investor discovers that the assets supposedly securing the investment do not exist, are worth much less than the investor had been led to believe, or were pledged to numerous other investors rendering them virtually worthless.
- The investor is often a financially unsophisticated individual who does not review the transaction papers in detail and may not understand them but is persuaded to invest by the prospect of a high return (for example, a well above average interest rate).
- The investor usually relies on the promises of the perpetrator or the apparent protection afforded by the security.

It should be noted that some assets pledged as security (that is, land or stock) may lose value for legitimate reasons such as fluctuations in their market values. In cases of false security, however, there is intent to deceive on the part of the person soliciting the funds.

Accounting evidence in most cases can establish and document the funds' flow in situations of this nature. It is more likely that evidence establishing the intent to deceive will be obtained by conducting interviews (*viva voce evidence*) than through the analysis of the accounting records. It is often through the interview process that the true nature and intent of the transactions are revealed. The nature of the documentary evidence required to establish the economic benefit to the fraud perpetrator, and to trace the flow of funds are dictated by the nature of the fraud scheme.

Trust Our Paper Inc. Case Study

Trust Our Paper Inc. commenced its syndicated mortgage program in 1995. The program expanded rapidly, particularly during 1998, to include loans for property development in Plainville. The company solicited—in appropriate private offerings—funds from the public for investment in specific mortgages, with certain representations made about the nature of each loan and the mortgaged property. Unbeknownst to the investors, the mortgaged property was not as marketable or valuable as had been represented because it did not have the necessary local governmental approval for development.

During 1998, the period of its most rapid expansion, Trust Our Paper experienced an increasingly severe negative cash flow from operations. This condition persisted until March 1999, when Trust Our Paper went into receivership primarily as a result of—

1. The apparent inability of the mortgagors (borrowers) to make interest payments.
2. The apparent inability of the mortgagors to pay principal amounts upon maturity.

In reality, the face amount of the mortgages were much higher than the underlying value of the property secured by the mortgages.

The problems in this case are best illustrated by a transaction that commenced in the summer of 1998, when Trust Our Paper purchased land in Plainville at a price of $400,000. It planned to build a 300-suite apartment complex on the land. Before the closing of the transaction, Trust Our Paper had been unsuccessful in obtaining mortgage financing through normal channels because of an inability to get zoning approval for its plans. The location of the land and environmental concerns proved to be insurmountable obstacles.

Trust Our Paper then provided a loan of $1 million to ABC Developments Ltd., the developer of the property, secured by a first mortgage on the property. Funds were solicited from the public—in a properly registered offering—for investment in this mortgage. Trust Our Paper represented to the investors that it had used the mortgage proceeds for interim construction of a 300-unit residential complex.

However, an examination of the mortgage proceeds revealed a different story. Out of the proceeds, $400,000 was used to reimburse Trust Our Paper for the cost of the property. Thus, the purchase was financed entirely by the investors through their loan to Trust Our Paper. Of the remaining funds, $115,000 was disbursed in November 1998 to Green Investments Inc., a troubled company with a deficit of $296,000. The balance of $485,000 was disbursed in a similar manner.

The underlying security given to the Trust Our Paper investors was highly questionable in light of the following:

1. The mortgage for $1 million was on land purchased for $400,000.
2. The mortgage guarantor advised that the property was unsuitable for financing.
3. The property remained undeveloped.
4. The developers were unable to obtain alternate mortgage financing.
5. The mortgage proceeds were not used as purported.

Thus, the proceeds raised from the public offering were diverted from their intended use, that is, to develop the property. This diversion diluted the value of the security and jeopardized the achievement of the appraised potential that was offered as security.

Advance Fee Fraud

Generally, advance fee schemes involve paying bogus corporations an up-front finder's fee in exchange for a promise to receive an advance on a loan. The victims of these kinds of schemes can be both individuals and corporations. Often if an individual is seeking loan funds but for whatever reason cannot obtain funding from traditional sources, he or she will turn in desperation to these fraudsters.

Once the fee is paid, the perpetrator disappears. In some cases, desperate institutions are offered access to illegal money, and they typically do not report the loss of the advance fee when the deal falls through. General characteristics of these schemes include one or more of the following:

- Deals too good to be true often are not true.
- The agent requests documents on bank stationery, or signatures of officers, or both.
- The bank is asked to give nondisclosure agreements to protect the agent or other parties.

- The agent asks for an irrevocable agreement to pay commissions, expenses, and a fee.
- There are several complex layers of agents, brokers, and other intermediaries.
- The perpetrators often describe the offerings as special *one of a kind* offers and state that the deal will be *killed* if anyone is contacted to verify the deal.
- The deal often involves foreign agents, banks, and other sources, such as an unnamed wealthy person or government.

Debt Consolidation Schemes

People who find themselves hopelessly in debt frequently turn to debt consolidation agencies out of desperation. Debt consolidation agencies do not advance loans, but rather act as an intermediary between the debtor and creditor. Some are legitimate, but many are not. Bona fide debt consolidation agencies make money by organizing the debtor's affairs and collecting a percentage of the money handled on the debtor's behalf.

In the typical scenario, the debtor contacts the consolidation agency, and provides a complete list of their creditors and the amount of monthly payments currently owed. The agency then usually writes letters to the creditors, requesting a debt work-out plan providing for lower monthly payments spread out over longer periods of time. The creditors are often motivated to accept the arrangement provided they think that the entire debt, or the major portion of it, will be repaid or that the debt consolidation plan will prevent a bankruptcy filing or default by the debtor. The debtor then makes a lump sum monthly payment to the consolidation agency, which then distributes the money to the creditors.

Unscrupulous debt consolidation schemes are perpetrated when the agency collects money from the debtor but does not forward it to the creditor. In some instances, it is months before the debtor finds out that the money has been misappropriated. The victim debtor has not only lost money to the unscrupulous agency, but still owes the original debt.

Bankruptcy Fraud

Bankruptcy is designed to give every corporation or individual encumbered by mountains of debt a *fresh start.* In a liquidation or Chapter 7 bankruptcy, all assets and liabilities are to be listed on the bankruptcy petition and a trustee is appointed by the U.S. Bankruptcy Trustee's Office in the district where the petition was filed. The role of the trustee is to liquidate the assets of the estate and distribute the funds to the creditors pursuant to the Bankruptcy Code.

Generally there are three common kinds of fraud committed by companies or individuals filing for bankruptcy; they are:

1. *Fraudulent conveyances.* Prior to the filing of the bankruptcy petition, cash or other assets are transferred to friends, relatives or business associates. Once the bankruptcy court has discharged the debtor's debts, these assets are then transferred back to the debtor. This kind of transfer is often referred to as *parking assets.* These prepetition transfers are often disguised to appear as bona fide business transactions.

2. *Concealing assets or asset stripping.* The debtor could: convert assets to his or her own benefit, simply fail to disclose certain assets in the bankruptcy schedules, or deny the existence of such assets when meeting with the trustee or at hearings before a bankruptcy judge.
3. *Planned bankruptcy.* The debtor's affairs are structured in a way that gives the appearance of a failing business, but is actually a lucrative business that needs to avoid the circumstances of a particular obligation, litigation, or labor dispute. This is often accomplished through the use of transfer pricing or management fees from related companies, which may or may not be disclosed to the trustee.

Planned Bankruptcy. Bankruptcy can be attributed primarily to one or a combination of the following causes:

- Incompetence of management
- Lack of managerial experience
- Neglect
- Severe economic recession or depression (macro or market sector)
- Disaster
- Fraud

Fraud is *not* the cause of most business failures.

The victims, regardless of the cause of a business failure, are customers and creditors: customers who have ordered or paid for goods that are undelivered at the time the business *goes belly up*, and the various creditors of the business that remain unpaid at that time. On many occasions the employees are also victimized because they lose their jobs or are unable to collect unpaid wages or both.

A business experiencing financial difficulties can pursue several remedies either to rectify the situation or to conclude the operation of the business. The owner may cease business voluntarily, or an unpaid creditor may precipitate the closing down of the business through the initiation of involuntary bankruptcy proceedings.

Ask the following questions when considering whether a bankruptcy was planned:

1. When did the company realize it would fail? A business failure may appear to be the result of management incompetence, inexperience and neglect. Notwithstanding the reasons for the financial difficulties, it is crucial to establish whether management carried on the business after a point in time when they knew, suspected or should have known that business failure was imminent. In that case, the fraud occurs when they solicit funds from the public, including creditors, in spite of knowing or suspecting that the company might be unable to fulfill the representations and commitments made. The business, however, may have continued in the honest belief that it would turn around (the *rainbow syndrome*).

   Establishing the point in time at which management knew, should have known, or suspected that business failure was imminent requires a detailed review and analysis of the financial position of the business. Financial statements, accounting records and banking records have to be scrutinized. (See Chapter 10 for further information on financial statement fraud.) The examination would disclose not only the financial position and any deterioration in it, but also the level of management's knowledge about the situation. Correspondence and other documents from customers and creditors, expressing concern or demanding delivery or repayment, together with viva voce evidence may also be useful.

2. Did the company pursue remedies? In determining whether fraud exists, the forensic accountant must consider whether the remedies available to the business in financial difficulty, as noted above, were pursued. In addition, the accountant must ask if honest attempts were made to resolve the difficulties or merely to give the impending business failure the appearance of legitimacy.
3. Has the business committed an act of bankruptcy? Bankruptcy law defines specific activities on the part of a debtor as constituting an act of bankruptcy. These activities include one or more of the following:
   - The transfer of assets to a trustee or other third party for the benefit of creditors
   - A payment to one creditor in preference over another
   - The fraudulent conveyance or transfer of property
   - An attempt by the debtor to abscond without paying debts
   - A failure to redeem goods seized under an execution order issued against the debtor
   - The presentation at a meeting of creditors of a statement of assets and liabilities indicating insolvency, or a written admission of the debtor's inability to pay his or her debts (the filing of a bankruptcy petition), or both
   - An attempt to move or hide any of the debtor's property
   - Notice to any creditors that the debtor is suspending payment of his or her debts
   - A failure to meet liabilities, generally, as they become due
   - Default in a proposal made as part of the bankruptcy proceedings
4. Was the business failure planned? A planned business failure occurs where management has converted the assets of the business to its own, that is, personal benefit and then tries to conceal the conversion through formal bankruptcy proceedings. In addition, the debtor induces vendors to sell goods on credit when the debtor knows that it has neither the intent nor the capacity to pay the creditors. Characteristics of a planned failure include one or more of the following:
   - The business has developed a reputation for trustworthiness in the business community. This reputation may have a short history, and may have been established for the express purpose of inducing companies to sell goods to the business on credit.
   - The business sells tangible and highly marketable products.
   - The business seeks to sell, or convert the goods to cash as quickly as possible with little care about the selling price because they have no intention of paying the suppliers for the goods.
   - The proceeds from operations are moved out of the business so as not to be identified as an asset of the business at the time of the filing of the bankruptcy petition.

- The business has little net worth.
- The business has not been a financial success.
- The business departs from its normal business practices with regard to purchasing, payments to suppliers, sales, and the granting of credit to customers.

The typical changes in business conduct of a planned failure include:

- The volume of inventory ordered from existing suppliers increases significantly. The suppliers will probably extend credit up to sixty days, largely as a result of their wish to retain the customer and the established reputation of the company.
- The unsuspecting suppliers will receive little or no payment. They may receive payment for the initial order but not for subsequent shipments. The scam will probably be completed within sixty days of the date of purchase of the inventory. After that time, the suppliers are likely to become suspicious and might take action of some kind.
- The company will refuse to sell the inventory to its customers on credit; that is, it will sell on a cash-on-delivery (COD) or other cash-up-front basis only. To get customers to pay cash, the selling price per unit is commonly at or below the company's cost price per unit, as shown on the supplier's invoice.
- If inventory still remains after the company has approached its usual customers, the inventory may then be offered to new customers. These sales tend to be non-arm's length and may be in cash. Although the sales invoices may indicate the payment was made in cash, the deposit of the cash into the business' bank account does not necessarily follow.
- If, after all these efforts to sell, inventory is still left at the site, it can be physically removed. The trail will be covered to prevent obvious detection.

A planned bankruptcy is designed, of course, to benefit those in control of the debtor entity. The fraudster will make every effort to ensure that no trail is left behind to enable the trustee in bankruptcy to retrieve the proceeds of the fraud and return those proceeds to the creditors. The techniques employed to block the path of the trustee are limited only by the perpetrator's imagination and will vary according to the circumstances.

7.2.4 Arson for Profit

Arson and a planned bankruptcy share some similar characteristics. In both situations, business problems exist and are acknowledged to exist by management. Arson, like planned bankruptcy, can become the means of a criminal making the best of a bad situation. The perpetrator will, of course, seek to commit the crime without leaving a trail of criminal conduct.

The following are the chief characteristics of cases of arson:

1. The fire is of an incendiary nature.
2. An insurance policy is in force.
3. There is a financial or other business-related motive.
4. The financial motive may not be readily apparent.
5. Exclusive opportunity to commit arson may or may not be evident.

6. The prosecution's case will often be based on circumstantial evidence.
7. Efforts may have been made to destroy some or all of the accounting and business records.

Without a confession or an eyewitness, the evidence in a case of arson is almost always circumstantial in nature. The prosecutor usually must depend on circumstantial evidence, which must be sufficient to rebut every reasonable hypothesis other than a willful and intentional burning. However, evidence supporting the incendiary origin of a fire is often interwoven with other evidence that tends to connect the accused with the crime. The connection to the accused is often the presence of a motive and the opportunity of the accused to perform the act.

Historically, insurance companies have been reluctant to challenge the veracity of loss claims arising from major fires that have damaged or destroyed commercial, industrial, recreational or residential establishments. The reasons given for this reluctance include the following:

- Court proceedings are protracted and expensive, and the ultimate decision is often favorable to the insured.
- The insurance company (like a bank) is often perceived as the *big, bad guy*, thus, the insured sometimes gets the benefit of reasonable doubt because they are perceived as the *little guy*.
- The punitive damages awarded to a claimant often far exceed the loss claim if the courts feel that there has been an unreasonable delay.
- The only evidence is circumstantial.
- The alleged arsonist has been acquitted in a related criminal proceeding.

Accounting Issues and Evidence

The forensic accountant in arson-related matters should differentiate the business position of the company and its owners from the financial position. Although the financial position may have a considerable bearing on motive, motive is better understood in the context of the business itself and the owners, through an overview of all aspects of the operations and ownership of the business.

Ultimately, the financial analysis is designed to determine the *mindset* of the company, the *money* of the company, and the *worker* in the company. Accordingly, it is usually appropriate to obtain as much background information as possible. A starting point may be the acquisition of a business or the commencement of a new business venture. A review of the annual financial statements and associated working papers will disclose the company's yearly performance and any underlying business problems. Motive not apparent from an analysis of the company's financial transactions may become apparent from an investigation of the social relationships found within a business.

Any review of the status of a business must be objective. It should identify not only matters that are unfavorable to management and the owners of the company, but also matters that are favorable. The unfavorable matters may well be obvious, for example, a steady decline in sales, worsening creditor relations, or a significant withdrawal of funds immediately before the fire. On the other hand, an owner may have put a substantial amount of his or her own money into the business shortly before the fire.

Accounting evidence is likely to be extremely significant in establishing motive. The fire may have destroyed some or all of the accounting and financial records, as well as correspondence and file material that could have a bearing on the case. These records will have to be reconstructed to the extent possible; thus, third-party documentation will have to be obtained and interpreted.

Issues and Sources of Information. A review of several recent judgments shows that the main characteristics in an arson investigation to consider, investigate, and establish in evidence are as follows:

1. Ownership, including business structure, style, and relationships
2. Financial motive, that is the financial position of the owners and business, and existence of an insurance policy
3. Current events at or around the time of the fire, including the establishment of exclusive opportunity, and the origin of the fire as incendiary

Information will be sought from people directly and indirectly connected with the business, possibly including its bankers, lawyer, accountant, customers, suppliers, insurers, government agencies, and realtors.

The owner should always be given the opportunity to volunteer any personal or business records that he or she might have.

See below for a list of questions to consider and documents to examine.

Accounting Evidence. Forensic accountants can assist by investigating several issues, in particular those involving ownership and financial motive. They can analyze information from several sources and construct a chronology of the financial events leading up to the fire. They can analyze the financial records of the owner, the business, and third parties, and demonstrate the company's position at the time of the fire, comparing it with earlier periods.

The forensic accountant looks for significant detail when attempting to determine whether a financial motive exists. If little or nothing is available in the way of accounting books and records and supporting documentation, the forensic accountant will pursue other third party sources to secure information for the examination.

Obviously, any financial and accounting records of the business that are available will have to be examined and analyzed. As previously noted, it is important to provide the owner the opportunity to volunteer whatever personal or business records he or she has. Beyond this, the forensic accountant will seek information from others directly or indirectly connected with the business.

Key questions to consider include the following:

1. What financial condition was the business really in?
2. Who maintained the accounting records?
3. What accounting records would have been available?
4. What is the ownership structure?
5. Is the financial position of the owner solid?
6. What was the business's cash flow?

7. Does the business support the owner?
8. Does the owner support the business?
9. Have the essential matters been established?
10. Is the potential defendant cooperative?
11. What is the history and pattern of earnings?
12. Could ownership benefit from *selling out* to the insurance company?
13. What did the owner know about his financial state at the time of the fire?
14. Did any significant events occur at or around the time of the fire?
15. Who are the major suppliers and what were the business' relations with them?
16. Who are the major customers and what were the business' relations with them?
17. Who are the bankers and what were the business' relations with them?
18. Who is the external auditor?
19. Who is the outside legal counsel?
20. Is the business for sale and are negotiations currently being conducted?
21. Have there been any recent changes in insurance coverage?

Third-party documents to investigate include:

- Government (usually the Secretary of State of the state of incorporation or of a state in which the corporation is registered to do business) business registration records
- Recorded documents (for example, for land or other property)
- Work papers and files of accountants, auditors, or both
- Any secured transactions registered under the commercial code of the relevant state
- Tax returns
- Correspondence with customers and suppliers
- Bank credit files
- Credit files from other creditors
- Bank statements, canceled checks, deposit slips, credit memos, and debit memos (paper or microfiche records)
- Payroll information
- General ledger records
- Real estate listings

7.2.5 Procurement Fraud

All organizations including manufacturers, financial institutions, governments, and retailers, as well as private individuals are involved in the procurement process to acquire goods or services. For each and every kind of purchased item, ranging from commodities and equipment to a professional's time via a consulting services contract, there is a different kind of procurement fraud that can be perpetrated by the provider of the goods or services.

The risks and warning signs associated with each kind of procurement fraud vary depending on what is being purchased, and also by the kind and stage of the procurement process: Questions to ask when examining procurement fraud include:

- Is the purchase competitive or noncompetitive?
- What pricing method was used: fixed fee, cost per unit, cost-plus, or a combination thereof?
- Did the fraud occur at the requirements definition stage, the bidding and selection stage, or the contract performance and evaluation stage?

Some of the more common kinds of procurement fraud include:

- Bid rigging or price fixing
- False invoices
- Inflated costs
- Product substitution
- Secret commissions and kickbacks

Bid Rigging or Price Fixing

Bid rigging or price fixing, is the process of setting the price or terms of the contract between the various bidders without the knowledge or consent of the purchaser.

For example, bidders on a highway construction project may secretly meet before bids are submitted. During their meeting, they decide who will submit the low bid and what the bid should be. They may also decide who will bid on what jobs. This is known as bid rotation.

Bid rigging is usually characterized by the lack of *independent* competitive bids, or by prices that are close together. The entity seeking the bids is victimized by having to pay higher prices than the amount that would have been charged had there been no collusion.

False Invoices

Invoices submitted by a contractor for goods that have not been delivered, or for services that have not been performed are false.

Inflated Costs

Contractors often use a pricing method in which they invoice on a cost-plus basis. That is, the contractor receives payment for the actual cost of the job, plus a certain profit based on a percentage of the costs. Clearly, the successful bidder has a vested interest in keeping the costs high: the higher the cost, the higher the profit.

Typically, in order to obtain inflated profits, contractors falsify the cost of the product or service. This can be done through simple or complex means. Examples of the former include adding labor charges for nonexistent *(ghost)* employees or adding charges for materials not actually used. In the more sophisticated schemes, the costs are inflated through overhead allocations.

Product Substitution

Procurement contracts sometimes call for very exacting specifications on the materials used on the job. Contractors frequently believe the contract specifications are too rigid and, therefore, feel justified in substituting a less costly product or service, and keeping the difference.

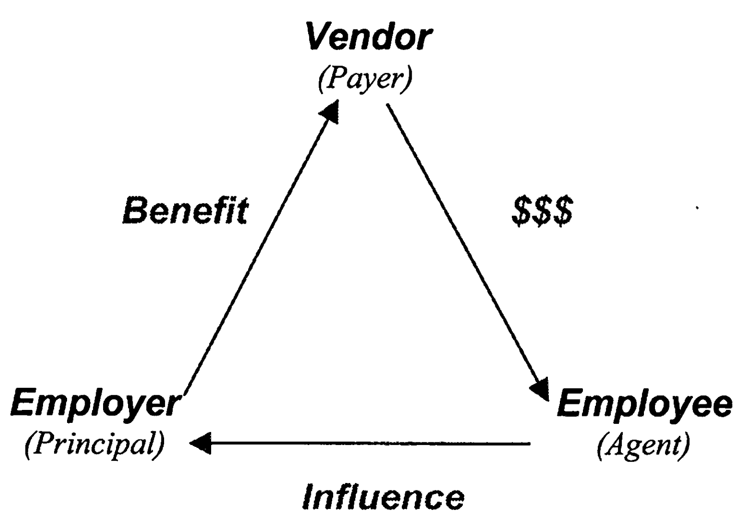
In one scheme, a contractor bid on a new runway for an airport authority and won the bid. The contract called for the depth of the concrete covering the runway to be a certain minimum. After hearing rumors from competitors that the contractor was pouring less concrete than the minimum, the authority's auditors checked the work orders and discovered that the paperwork reflected the concrete depth to hundredths of an inch. The auditor reasoned that concrete could not be poured so exactly, checked the actual work, and found the depth to be less than the contract specifications. The auditors concluded that the contractor was submitting false reports to the airport authority, and was reaping excess profit because it was supplying less material than that called for in the contract.

Secret Commissions and Kickbacks

Secret commissions and kickbacks are one of the most common forms of procurement fraud, and also one of the most difficult to detect. It involves the receipt of a secret payment, usually from one company (the vendor-payer) to a corporate executive (the agent) of another company (the procurer): the agent then exercises influence on the decision-making of his or her employer in a way that favors the vendor-payer. For example, a vendor submits false or inflated invoices for payment, which the procurer's corporate executive knowingly approves. This process is often described visually by the triangle of dishonesty shown in figure 7-1.

The key point to note is that secret commissions and kickbacks are a kind of fraud that generally accompanies other forms of procurement fraud (such as those described in this section).

Figure 7-1. Triangle of dishonesty



7.2.6 Organizational Bribe Giving

The two main kinds of bribes that benefit organizations are:

1. Bribing politicians and giving illegal campaign contributions.
2. Implementing commercial bribery as related to procurement fraud. Also included here are bribes for industrial espionage—that is, paying someone to reveal trade and other secrets about competitors.

Political Bribery

There are three generally recognized characteristics of political bribe giving:

1. Government benefits are often extremely valuable (or, for penalties and sanctions, very costly), but the demand for benefits can exceed the supply.
2. The government is the sole purveyor of the benefits and sanctions; you must do business with the government.
3. The bribe is an attempt to both bypass and guarantee the result of the normal processes, which are often lengthy, costly, and uncertain in result.

The most common form of political bribe giving is illegal campaign contributions, which have made headlines during the Clinton Administration.

Paying foreign politicians and governments was (and perhaps still is) common in order to conduct business in many countries. Since the mid-seventies, when the Foreign Corrupt Practices Act was enacted, paying bribes to foreign officials except in cases of national security has been unlawful.

Commercial Bribery

Commercial bribery involves making payments in exchange for the award of a contract, for industrial espionage, or for both.

In the triangle of dishonesty, a payment from a vendor to an employee would encourage the employee to influence the decision regarding the recipient of a lucrative contract.

Several federal and state laws address the practice of commercial bribery. Both the act of asking for or the making of a payment constitutes an offense. In some instances commercial bribery may also be a violation of the restraint-of-trade laws. For example, certain industries—notably the liquor industry—are specifically prohibited from paying for business. Over the years, many well-known, major businesses have been guilty of commercial bribery (a listing of names would not add learning other than the giants of industry are involved from-time-to-time in nefarious activities).

Industrial espionage can involve direct payments to third parties to secure valuable competitive information. It can also be accomplished indirectly, for example, through the hiring of a competitor's employees. In one case, several U.S. military procurement agents were charged with giving defense contractors information on more than $500 million in Navy purchases that were going to be the subject of the competitive bidding process.

7.2.7 Industrial Espionage

Industrial espionage is a term that is broadly applied to activities whose main purpose is to obtain information or related assets from competitors or potential competitors. The classic forms of industrial espionage are trade-secret theft and copyright piracy.

Trade Secrets

There are three basic elements to a trade secret: novelty, value, and secrecy. Secrecy, concerns whether an organization handled its alleged *secret* in a protective manner. If a judge deems that an organization failed to protect a secret, that organization will not win judicial support if it charges an employee with theft of that secret.

Patent laws seek a compromise between capitalistic self-interest in a trade secret and social well-being by granting a seventeen-year monopoly to developers of innovative ideas. The U.S. Supreme Court, in its only ruling on trade secrets (*Kewanee Oil Co.* v. *Bicron Corp.*, 1974), declared the likelihood "remote indeed" that a company would not patent valuable information that it had developed. However, the Court overlooked the advantage, well-known to most companies, that trade secrets can be hoarded far beyond the seventeen-year patent limitation, a matter well documented by the success and secrecy of the formulas for Coca-Cola and Kentucky Fried Chicken, among others.

Leakage of trade secret information is said to be particularly likely from employees who go to work for competitors, careless secretaries, gregarious field sales personnel, and high-tech computer whizzes who often are more loyal to their equipment than to their fellow employees or employer. Temporary help is regarded as especially vulnerable: these employees do not have any company loyalty and can be planted for purposes of trade-secret theft. Sharing sensitive information among two or more individuals, neither of whom knows the full *secret,* is one way to reduce the possibility of compromising sensitive information. Another method can be used to protect mailing lists. By including at least one decoy address in a list, if the list is compromised, whoever uses it will be sending material to a fictional person at an address that actually is the list-owning company's mail drop.

A review of court cases on trade-secret theft shows that defendants are typically smaller corporations that have hired scientists from larger organizations where they had previously worked for six to ten years. There also appears to be an unusual amount of trade-secret theft from family-owned businesses. The defendants in these cases claim that because they were outsiders, they believed their chances of advancement were hopeless, so they stole the proprietary information to benefit (ingratiate themselves with) their new employers.

Copyright Piracy

Copyright piracy is defined as the infringement of another's copyright or other business rights. It is an activity usually undertaken by manufacturers, wholesalers or retailers that do not have any legal right to manufacture or copy the product, but who want to earn a quick profit (greed motive) or to ease a financial difficulty (need motive).

Bigtown Video Case Study

From August 1997 to May 1, 1998, John Smith was the owner, principal shareholder, director, president, and general manager of Bigtown Video Inc., a video store with three retail outlets. During this time Jack Brown was also a shareholder and secretary-treasurer of the company.

Bigtown Video's business included the sale and rental of prerecorded videocassettes as well as the sale of blank cassettes. The videotapes sold and rented by Bigtown Video fell into two categories: legitimate and "counterfeit." The legitimate tapes were obtained from sources authorized to manufacture and distribute the tapes in compliance with all copyright and distribution rights. They were packaged with stylized printed jackets showing the nature and content of the particular film. The counterfeit tapes had been duplicated from legitimate tapes, many of which had not yet been released to the public in videocassette form. The packaging of the counterfeit tapes was like that of a blank cassette package with the title of the film handwritten on the side panel. The legitimate tapes were displayed in the front of the stores. The counterfeit tapes were kept in the back rooms of the stores in a closet or in a drawer.

When cross-examined at trial, Mr. Brown testified that he and Mr. Smith had jointly decided to deal in counterfeit videocassettes in late 1997. The decision was made as a result of customer demands and financial difficulties. Mr. Brown would buy counterfeit cassettes from various sources and make duplicates of them. These actions were done with Mr. Smith's knowledge and consent. Mr. Smith rented the counterfeit videocassettes at rates of $5 or more and sold them for prices ranging from $60 to $100 or more. From January 1998 until May 1998, the gross profit made by the company from each of the three stores was approximately $1,500 per week, of which about 60 percent was attributed to the distribution of the counterfeit videotapes.

In Mr. Smith's cross-examination, he revealed that he was fully aware of the illegitimate origins of the counterfeit videocassettes supplied to him and that neither he, his suppliers, nor Bigtown Video had the right to distribute, rent or sell the cassettes. Mr. Smith knew that by dealing in these counterfeit tapes he was effectively depriving their owners of copyright and distribution revenues, which they would otherwise have been likely to earn but for the use of these illegitimate tapes: he was prejudicing the economic interests of the real owner. Mr. Smith made no attempt to contact the owners of the copyright or distribution rights in order to contribute revenues for his counterfeit use, to obtain these rights, and he had no intention of so doing.

Bob Green, a vice-president at Star-Studded Studios, testified about the effect of pirated videocassettes on the revenues of his company. He focused on four areas of impact and said:

1. That the inferior quality of pirated or counterfeit videocassettes tends to provide the viewer with a poor opinion of the film and the consequent negative publicity is harmful to the theatrical market.

2. That people who have seen a counterfeit videocassette are unlikely to buy the legitimate cassette upon its release.
3. That for extremely high-grossing films, much of the profit arises out of repeated viewings of the film by the public. The effect of a counterfeit videocassette in such a situation is to diminish the theatrical value of the film by eliminating the possessor's desire to return to the theater.
4. That with respect to distribution in other territories, the markets for legitimate cassettes have vanished due to the heavy influx of counterfeit videocassettes in those territories. In cross-examination Mr. Green admitted that he could not quantify the loss of profit by theatres from counterfeit videocassettes, nor could he reliably estimate the extent of loss for a given film or a given year.

7.2.8 Securities Fraud

There are four main kinds of securities fraud that fall within the category of commercial crime:

1. Knowingly providing misleading or false information in financial statements of a traded business enterprise. (See Chapter 10 for further information on financial statement fraud.)
2. *Churning*: An activity of brokers who buy and sell their clients' securities for the sole purpose of generating commissions.
3. Mixing (commingling) of funds.
4. Manipulating the market for a stock by altering the stock's price through influencing the factors that affect the market price or by controlling the pool of shares available for sale or purchase.

Misleading or False Financial Statements

In large companies, upper level management, whose intent is not necessarily to steal, often manipulates financial statement information. These managers wish to manipulate data to enhance profitability and thereby earn higher bonuses, or to impress the brass at headquarters, or to impress stockholders or lenders, or simply to comply with the goals imposed by senior management. In small companies, where false financial results can create a direct benefit for senior management, the intent of management is often sinister.

Intentionally falsifying financial statements can be accomplished by one of the following methods:

1. Misstatement of financial information by arbitrarily raising profits or lowering costs using techniques such as plugging sales or ending inventory, incorrectly capitalizing current expenses, deferring necessary repairs, falsifying sales invoices, and altering cost invoices.
2. Misrepresentation or omission of significant information.
3. Misapplication of accounting principles.

In the MiniScribe fraud, the company knowingly inflated inventories to deceive the auditors as to the value of assets on hand; the primary goal was to maintain and drive the share price of the company up in the public market.

In more recent instances, particularly in the high tech environment, *channel stuffing* (that is, just before year end, shipping inventory to distributors and dealers whether or not ordered, and booking the shipments as sales) was a popular method used to inflate sales to achieve projected and expected revenue goals. In many instances, product recorded as sold was returned shortly after year-end.

Heinz Catch-Up Case Study

Heinz has been a household name representing quality food products for more than one hundred years. The company had been well managed, profitable and socially responsible. But in the late 1970s, it received considerable unfavorable publicity for accounting irregularities. Some of its profit-center managers engaged in reducing its profits to create a cushion for the next year. The total amount of these pseudo-profit reductions was quite small ($8.5 million) when compared to overall sales ($2.4 billion). However, annual sales and profits were not what were reported to the IRS, the Securities and Exchange Commission (SEC), and company stockholders.

The disclosure of these irregularities occurred as a result of an antitrust suit brought by Heinz against Campbell Soup. In Campbell's discovery efforts, it snagged evidence that Heinz' advertising agency was billing for services that had not yet been rendered. When a Heinz executive was questioned about the matter, he pleaded the Fifth Amendment.

The antitrust suit was settled shortly afterwards, but the disclosure caused Heinz headquarters' personnel to launch an investigation into the accounting practices of several subsidiaries. Being highly decentralized, headquarters' personnel claimed they were unaware of the lower-level fudging. Headquarters monitored performance through budget forecasts of sales and expenses and an incentive compensation plan that paid off if high-end profit goals were met. Headquarters also monitored consistent growth in profits. Top management was committed to that overriding goal and, the company's earnings did rise consistently: for example, 1978 marked the fifteenth consecutive year of record profits.

Heinz had an explicit policy that prohibited its divisions from having any form of unrecorded assets or false entries in its books and records. And Heinz didn't measure short-term performance alone. The top nineteen executives, including division general managers, had long-term incentive plans in addition to the one-year plan.

What existed here initially were income transferals aided and abetted by vendors who supplied invoices one year for services that were not rendered until the next year. When that wasn't enough, false invoices were submitted one year and then reversed in the following year. But the amounts involved did not have a material effect on the company's reported profits.

Strangely, the problem at Heinz started in 1974 when it appeared that profits in the Heinz USA division would exceed those allowed by the wage and price controls in effect at the time. World headquarters sought a way to reduce the division's profit. Losses in commodity transactions did not reduce profits enough, so the division booked $2 million in advertising services. Yet, instead of treating the expense as a prepaid item, the company charged the advertising expenses off immediately. Despite the lower profits of the division, world headquarters decided that the division had achieved its goal and paid the relevant bonuses.

By 1977, the following practices had evolved at the Heinz USA division:

1. Employees delayed year-end shipments until the beginning of the next year to ensure accurate invoicing dates.
2. Employees handled customer complaints about the delays by making the shipments, but misdating the shipping and invoice documents.
3. Employees did not record credits from vendors until the following year.
4. *Income management* became a way of life. One employee was given the task of maintaining private records to ensure the recovery of amounts paid to vendors on improper invoices.
5. The practice of delayed shipment and prepaid billing to assure that departmental budgeted amounts were met permeated the division down to the departmental level.
6. Ten separate vendors joined in supplying improper invoices.
7. Employees used other questionable tactics to manipulate income including inflated accruals, inventory adjustments, commodity transactions and customer rebates.

What can be learned from this case? First, exerting pressure for continuous growth in profits may foster improper accounting practices, particularly if coupled with an incentive compensation plan that rewards and reinforces continuous growth on the high side. Second, autonomous units with independent accounting capabilities might be tempted, under the above circumstances, to manipulate performance data.

Heinz isn't the only case in which autonomous accounting or pressure for performance led to manipulations of records. There were similar episodes in the 1980s at McCormick and Company, J. Walter Thompson, Datapoint Corporation, Saxon Industries, Ronson Corporation, Pepsico, AM International, U.S. Surgical, and Stauffer Chemical. More recently, companies like Sunbeam and Cendant have been in the news for the same kind of earnings manipulation.

Churning

Churning occurs when a broker buys and sells stock for a client to generate fees, rather than to protect the best interests of the client. Broker discretionary accounts are especially ripe for churning because they can be used to generate fees for both the brokerage firm and the broker, without much involvement or control by the actual investor.

In one case, two sisters gave brokers $500,000 each to be held in discretionary brokerage accounts. The brokers executed more than 1,400 stock trades, allegedly earning themselves $400,000 in commissions, while leaving the sisters with $70,000.

Mixing of Funds

Another scheme involves mixing (commingling) client funds with the funds of the brokerage firm, or broker, or both. In these cases, brokers will use the client's stock as collateral for corporate or personal loans, and post the winning trades to themselves, while posting the losses to their clients. Some brokers also resort to out-and-out embezzlement of their client's money and stock.

Manipulating the Stock Market

Stock market manipulation is a crime perpetrated by a promoter who artificially influences the market price of shares in a company for self-benefit or for the benefit of his or her holding company at the expense of the investing public. In most cases, the promoter flogs his or her holdings to the public, the public pays an artificially high price for the stock, and the resulting increase in price lines the pockets of the promoter.

Promoters of the stock are usually self-styled financiers who start off owning the majority of the stock. Often other conspirators join the promoter, forming a control group consisting of financiers, warehousers, or brokerage salespersons, some or all of whom might be acting under a corporate umbrella.

To increase the stock's price, the promoter subjects it to a multipronged attack. The promoter uses such weapons as influencing the demand for the stock and controlling the supply of the stock, warehousing the stock (parking), paying secret commissions, wash trading, and issuing fictitious press releases, all of which are intended to stimulate more trading than would otherwise occur.

The victim is the investing public. In many ways this particular fraud is similar to other investment scams that rely on telephone solicitations (boiler room operations) and high commission rates (which are often secret).

Reasons to Study This Kind of Crime. It has been argued that stock market manipulation is a very specialized kind of crime, restricted to the larger financial centers and, therefore, few CPAs are likely to come across them. Nevertheless, because of the great increase in stock market investments, residents anyplace in the country may become victims of stock market manipulation and may look to their CPA for advice. Further, an increasing number of CPAs are providing financial planning services, including investment advisory services, to their clients. These CPAs must be aware of stock manipulation schemes to protect both their clients and themselves.

In addition, stock market manipulation and the *modus operandi* may resemble other kinds of scams in which the price of an investment is influenced by the laws of supply and demand. Therefore, CPAs should be aware of this kind of crime. They could be called upon to speak to the public about prevention of white-collar crime in general or investment scams in particular. Also, they may become an investor in the stock market themselves.

Possible Red Flags. Red flags possibly signaling stock market manipulation, with the possible exception of churning and commingling of funds, are not as readily apparent as they are in some other kinds of economic crime. Most red flags seem to originate from an informant close to or aware of the control group. In contrast, the regularly required reports investors receive should be reviewed on receipt to assure that there are not patent red flags, that is, there is no churning or commingling of funds. Of course, if the fraud involves falsifying these reports, discovery will probably be delayed until the fraudster is caught, by which time, the investor could well be wiped out.

The SEC and stock exchanges usually carry out investigations to detect this type of crime and the investigations are mainly analytical. Unusual price increases or large commissions earned by salespeople may be investigated, as may press releases or assets reported on financial statements.

Price as Determined by the Law of Supply and Demand. The law of supply and demand states, in essence, that the price of an item will rise when demand for the item exceeds the available supply of that item, and the price will fall when supply exceeds demand. Throughout a stock manipulation, the promoter attempts to control both the supply of, and the demand for, a stock in order to move the price higher. As supply is restricted, the price increases. As demand is stimulated, the price increases.

A stock market is a composite of the interests of many individuals and corporations offering to buy and sell shares. Individuals, however, are influenced not only by information (whether accurate or not), but also by motives such as greed or fear and by perceptions that may have little to do with facts or reason. Investors are capable of changing their investment decisions quickly, purchasing recklessly in a down cycle or staying out of the market entirely in anticipation of disappointing financial information. The common desire is to make profits and to prefer investments that are perceived as likely to produce profits, whether or not these perceptions are based in reality.

Thus, investors will often overreact in seeking to take advantage of price changes or in attempting to correct their errors. A single item of speculative news may dramatically change the number of people who are willing to purchase, hold or sell a particular investment, dramatically changing the demand for the shares. It is important to note that large volumes of shares are often exchanged. Accordingly, time is of the essence in keeping losses to a minimum and gaining the greatest possible profits. Precisely when a buy or sell transaction takes place can make a big difference in the value of the purchase or sale.

Market prices are generally influenced by the release of corporate information, such as news about profits, the announcement of a new product line, or the discovery of a new oil reserve, as well as by changes in government policy, forecasts, prospectuses, and in general, matters that occur in the ordinary daily conduct of a business.

In summary, the investing public, through the medium of publicly held stock, whether traded on an exchange, the NASDQ or over the counter, is able to place a value on a share and to decide to buy or sell accordingly. As more people seek to buy shares, the price of a share will increase if the number of shares for sale on the market remains the same. Conversely, the price will fall if an excess supply of shares is available or if the public demand for the shares drops.

The Manipulation Process. Generally, a manipulation begins with the promoter falsely increasing demand and restricting or controlling the supply. The combined effect of this process is an increase in price. After a certain point, called the *blow off*, the promoter attempts to increase supply and dampen demand in order to reduce the price, allowing the promoter to repurchase at a profit. Throughout, the promoter must act as a control valve in releasing the stock in order to control the market price, and hence the profits.

Manipulation may be motivated not only by a promoter wanting to make more money, but also by the desire to make the asset side of an investor's balance sheet look good or to improve the performance of an investment portfolio.

A promoter may use any combination of the following tactics to encourage the public to buy stock at higher and higher prices:

- Using buy or sell pressure by stock brokers who may be receiving secret commissions
- Distributing false press releases and rumors
- Releasing false ownership information
- Promoting fictitious or grossly exaggerated profits, assets or future prospects (or any combination thereof)
- Warehousing to help restrict the supply of shares
- Using wash trading (that is, trading that results in no change in beneficial ownership) to stimulate public interest due to high trading volumes
- Controlling the first or last trade of the day in order to set the highest possible price for the stock
- Dumping into foreign markets

Some or all of the activities generally used in the manipulation process are shown in figure 7-2.

Figure 7-2. Activities frequently used in the cycle of manipulating the stock market

Price Increase: ↑	*Price Decrease:* ↓
• Obtaining control	• Backdooring
• Setting up a distribution network	• Blowing off
• Warehousing	• Short selling
• Using wash trading	• Issuing bad news releases
• Issuing good news releases	• Repurchasing

A promoter who wanted to manipulate the price of a stock might use any combination of the activities listed below

1. *Obtaining Control*: The first step that a promoter usually takes is to gain control over an existing company's shares of stock to ensure that the public's selling off large quantities of the stock does not undermine his control over the supply of shares. Generally, 70-to-90 percent of the voting shares that are issued and outstanding must be acquired to exert effective control. The promoter can gain the necessary control by using one or a combination of the following:

- Buying the shares of an inactive company that is already listed on an exchange (commonly known as *cleaning up the market*). The shares of the promoter's unlisted company (which do not meet the requirements for listing on an exchange) can then become listed by merging the corporations and exchanging the unlisted shares for shares of the listed company.
- Buying a shell company that may have been inactive for a number of years.
- Underwriting an issue of new shares of a somewhat controlled company. This underwriting usually consists of a new issue of shares in an amount that far exceeds the original number of outstanding shares. To a promoter, this is the least desirable method, as it requires a prospectus, financial reporting, and an insider trading report. In addition, the promoter will have to arrange for his friends to purchase the new shares and hold them (park them) on his behalf an unequivocally fraudulent transaction.

2. *Setting up a Distribution Network*: A distribution network is set up with the promoter at its head. Immediately underneath the promoter are several distributors in cities that have stock traders or brokerages. Each of these distributors has access to a brokerage house's salespeople who then have access to the active traders. Via this network, the promoter now has control over what happens in the promoted stock's market. Secret commissions are sometimes paid to ensure that the network complies with the promoter's demands.

   The traders let the salespeople know when trades are pending and keeps them informed as to the price movement of the promoted stock so that the promoter can take compensating action. The salesperson's job is to give the public a sales pitch as to why they should buy the stock and, once in, why they should stay in. In addition, the salesperson's activity will affect the daily trading volume. What members of the public do not know in this situation is that the shares they are purchasing are those of the promoters.
3. *Warehousing*: Warehousing places shares into the hands of people who are friendly to the promoter. This is essential in order to maintain control of the shares and continue to restrict and regulate the supply of shares available. This is often accomplished by having friends buy new offerings of the stock and continuing to hold these shares until the promoter instructs them to sell.
4. *Wash Trading*: To promote the public's interest and increase demand for the promoted stock, the promoter manipulates the volume of stock traded through wash-trading. Essentially, this procedure consists of a stock purchases and sales with no change in beneficial ownership. Wash trading can be accomplished through nominee accounts: accounts at banks or trust companies set up under the names of trustees, friends, aliases, or false company names. The promoter sells a block of shares and at the same time a nominee enters a buy order to match the sell transaction. While the stock is kept out of the public's hands, this active, ostensibly normal trading is reflected in the volume numbers the public sees. Hence, the market in the manipulated stock appears to be an active one in the public's eyes.

5. *Issuing Good News Releases*: One or more timely news releases may be issued to promote the stock, attracting further public interest. The news releases may include verifiable information but may also consist of unsubstantiated rumors, such as:
   - Anticipation of good results from drilling tests in resource-based companies
   - Expectations for a likely acquisition of rights to explore property close to existing known resources
   - Plans for diversification into a *glamour* industry

   Generally the good news may be described as an intangible promise of future results. There is nothing of immediate value today. These good news releases are designed to stimulate the public interest and encourage them to buy shares, even at a high price.
6. *Backdooring: Backdooring* occurs when friends operating as a warehouse, which the promoter has previously set up, start selling their shares while the price is still increasing—contrary to their agreement with the promoter—before getting the word from the promoter to sell. The friends are backdooring the promoter, effectively double crossing the promoter. In order to sustain public demand, the promoter has to buy the backdoor shares at the market price if the existing public demand is not sufficient to support these sales.
7. *Blowing Off*: After the promoter has successfully stimulated demand, members of the public buy significant numbers of shares and then wait for the price to continue its anticipated rise. The promoter has already picked a tentative price at which he wants to dispose of his holdings. He starts selling his shares, as well as those of his nominees and friends. In these circumstances, the sale of unusually large amounts of stock is referred to as a *blow off*. The public, expecting a continued price rise, buy the promoter's shares over a relatively short period of time.

   The price at which the promoter actually begins to blow off his holdings depends primarily on how much public demand the distribution network has created and how long the demand is sustained. By blowing off, the promoter has withdrawn all active support of the stock price. He ceases wash trading, the reported trading volume decreases, and the price begins to fall quickly as supply far exceeds demand.
8. *Short Selling*: Short selling is the act of selling stock that one does not yet own and is a legitimate market activity. The seller is gambling that the price will decrease and that he or she will be able to buy back the shares at a price lower than the current-selling price. In this situation, the promoter can safely sell short, because he or she knows that the price will go down. Thus, the promoter realizes a profit both as the price of the stock goes up and again as the price goes down.
9. *Issuing Bad News Releases*: At this point, the promoter often issues a news release about the company's misfortunes. The exact reverse of the good news release, the promoter intends the bad news release to drive down the price of the stock rapidly.
10. *Repurchasing*: The stock price has now reached rock bottom, and the public is willing to sell at any price. The promoter often buys back control of the company when the shares reach this low price and changes the name of the company in order to start the process again. The same company, under a new name, will go through the cycle again in a period of one to two years.

Secret Commissions. Secret commissions were previously mentioned in the distribution network discussion. Generally, secret commissions or bribes are given to people in the securities industry to induce them to push or promote the shares in the promoter's company and to advise the promoter of orders to purchase shares before the orders are entered. Secret commissions may also be paid to the wash traders in order to keep their support. Generally, secret commissions are paid in one or more of the following ways:

- By a check drawn on either a personal or a corporate bank account and payable to the recipient, to cash, or to a third party. If the check is paid to a third party, it will be endorsed by the named third party and cashed, with the cash being passed on to the true recipient of the secret commission.
- By a free delivery to the recipient of stock in signed-off or *street certificate* form, which can then be sold by the recipient on the market.
- By the issuance to the recipient of call options on the stock at a fixed price below the current market price.
- By selling a block of stock to a salesperson or another recipient at a fixed price and allowing that buyer to sell that block back at a higher price.

The Significance of Accounting Evidence. Accounting evidence is generally very significant in the prosecution of stock market manipulation cases because—

- The accountant can perform an analysis to determine whether change in beneficial ownership occurred (a wash trading analysis).
- Accounting evidence may be instrumental in identifying payments or receipts of secret commissions, if any.
- Accounting evidence can be used to establish the percentage of the public's participation in buying and selling shares when compared to the total transactions in the stock by the control group.
- Accounting evidence may assist in establishing that the perpetrators have benefited from the sale of the stock.

However, accounting evidence may not be as significant as *viva voce* evidence in initially identifying the control group, establishing the secret commission structure, and identifying who was paying and receiving these commissions.

Possible Preventive Measures. Perhaps the most significant stock manipulation preventive measure is to make the investing public aware that a salesperson's pitch will be persuasive, will play on the investor's greed, and will convey a sense of urgency. The following are questions that an investor should ask a salesperson to answer on the record concerning the specific representations being made about the investment. The answers given should help in identifying poor or fraudulent investments.

1. How risky is this stock?
2. What direct costs are paid out of the investors' funds, such as for commissions, or advertising, or both?
3. Can I get written documents (the prospectus at a minimum), and can you mail them to me?
4. What is the specific destination (that is, bank account, brokerage account) of my funds?

5. How can I sell the stock if I choose to do so, and how long will it take to dispose of the investment?
6. What are the names of the principal owners and officers of the salesperson's firm, and what are the names of the owners and officers of the company in which the investment is being made?

Gonna Put You in the Movies Corp. Case Study

In early 1998, Jack Smith started to promote a company called Acme Mines Co., a shell company listed on the Westville Stock Exchange. Smith had effective control of the outstanding shares. In order to promote public interest and buying, Smith made announcements—through investor bulletins and statutory statements to regulatory bodies—to the effect that Acme was about to diversify into the movie production business and other ventures. The announcement touted:

- An investment of $175,000 in the production of a movie, which would return 25 percent of the profits to Acme
- A purchase yielding 58 percent control of a movie theater business called Everytown Theaters Ltd.
- An acquisition of distribution rights to *Krazy Kandy*, a confection that would be sold from automatic vending machines across the country

On February 4, 1998, Smith changed the name of the company from Acme Mines Co. to Gonna Put You in the Movies Corp. (GPY-Movies) to reflect its new objectives.

Smith's next step was to stimulate trading activity in GPY-Movies' stock on the Westville Stock Exchange. To accomplish this, offices were maintained in Bigtown and Westville and were operated by Mike Jones, a securities desk-trader, and the controller, Dave Brown. Their objectives appear to have been to maintain the market with effective control, match orders to create activity (wash trading), and systematically sell off the stock for profit.

Smith would tell Jones when to buy or sell. Jones would follow through via a series of controlled nominee accounts. Brown's job was to keep track of all the accounts, meet corporate requirements, and generally manage the money and the office in Bigtown. The nominee accounts were all in corporate names and could be traded by Mr. Smith, Mr. Jones or Mr. Brown.

The office in Bigtown was in the name of Anyco Investment Corp. The accounts at brokerage firms in both Westville and Bigtown were in the following names:

1. Metro Trading Associates.
2. Oakville Investments Co.
3. Pineville Trading Ltd.
4. Anyco Investment Corp.

At this time Smith was either an officer or director of each company and effectively controlled them. Stock positions in GPY-Movies were established through numerous Bigtown and Westville brokerage firms.

The eventual objective was to sell off or distribute the stock for a profit without causing an obvious decrease in the market price. To achieve this goal, Smith hired Robert Green who started to work out of the Bigtown Office around April 2, 1998. Smith instructed Green to sell stock through the accounts of Anyco and Metro Trading and to limit the price to $1.26 until an underwriting was effected, which was to occur on April 18, 1998.

Green's procedure was to prearrange all the buy orders so that they could be matched with any one of Smith's selling accounts. Whenever Green learned of a buy order, he would notify Jones of its size, price and the name of the brokerage firm. This meant that Green had to be in contact with sales reps or their distributors who would notify him of forthcoming buy orders. In order to secure their cooperation, Smith specifically authorized Green to pay sales reps a 15 percent commission over and above the amount sales reps would normally receive. In addition, Green, with the assistance of Smith and Brown, arranged for Wally Chang, a brokerage house manager, to use his sales force to distribute 300,000 shares of GPY-Movies throughout the United States for a 12½ percent commission.

On occasion, Smith arranged to provide cash to Green in order to make payments to sales reps. Brown made the checks payable to cash and drew them on one of the companies' accounts. Green made his own arrangements as to where and when to pay the sales reps.

Smith convinced two sales reps, Black and White, to set up an account in their firm. Whenever Black and White were able to persuade one of their clients to buy GPY-Movies shares, the offset would come out of Smith's account in the name of Metro Trading. In this way, Smith was able to sell off his position and pay Black and White with shares that they in turn sold through nominee accounts. Paul Wilson, an analyst, provided Smith with inside information on who was bidding or offering, as he was indebted to Smith for a substantial loan.

Thus, Smith and Jones, in an effort to generate personal gain, created a misleading appearance of active public trading in shares of GPY-Movies, both by wash trading and by the use of secret commissions. The result was a loss to the investing public.

7.2.9 Environmental Abuse

Generally there are two main kinds of environmental abuse that a company can commit:

1. Pollution
2. Misuse of natural resources

Pollution

While a certain level of pollution is tolerated by today's society, media attention has recently focused on companies that have gone too far. Society is, as a whole, becoming less tolerant of all forms of pollution, and this is reflected all the way down to the consumer—for instance, aerosol spray cans and cigarette smoking in restaurants are no longer tolerated in many jurisdictions. Laws have been passed to limit the levels of pollution, but not all companies comply with the laws, usually because of the added costs incurred.

Amount of Pollution. The amount of pollution and how it is determined depend on the nature and source of the pollution. For example, a perpetrator may have dumped garbage at an authorized site but in quantities greater than the dumping license permits. Or, a perpetrator may have dumped garbage at an unauthorized site. Or, a perpetrator may have polluted the environment in some other way, for example, dumping toxic substances into a river, or exceeding the specificed limits of emission of certain substances into the atmosphere.

Regardless of the nature and source of the pollution, the alleged offender's accounting and administrative records are likely to yield pertinent information about the physical quantities of substances that are themselves pollutants or that result in pollution. Financial records can also provide useful evidence as to the alleged offender's knowledge and intent. For example, an accounts receivable listing would reveal the names of the company's customers, but additional documents would be needed to assess the extent of the polluting activities. These documents might include invoices, bills of lading, weigh tickets, contracts, production reports, and so on.

Depending on the nature of the abuse, the financial records may help to put a dollar value on the cost of the damage done. For example, if you can establish that a company dumped in excess of the 5,000-ton-garbage limit permitted by its license, the courts can calculate the cost of the excess from the company's accounting records. This *cost* provides the judiciary with a yardstick against which to determine damages.

Dumping Unlimited Case Study

Dumping Unlimited was a carting company that had a license to dump waste material at a landfill site near Anytown. The company's license permitted dumping a maximum of 150 tons of material per day at the landfill.

Dumping Unlimited maintained a fleet of garbage trucks, which dumped the company's waste at the landfill site, and they also accepted waste material from other haulers on a daily basis.

Based on an analysis of weigh tickets, it was clear that the company was dumping quantities in excess of the permitted amount. To determine the value of these quantities, the excess tonnage was priced at the highest and the lowest price charged by the company, giving a range of values attributable to this offence.

Financial Capacity. Companies that are fined for noncompliance with antipollution laws often claim that they cannot afford either the costs of compliance at the time when the pollution was generated or the costs associated with cleaning up the after effects of the pollution.

Both of these issues are best examined by a CPA and involve examining financial statements and budgets.

There are relationships between various components in the financial statements, which help to identify historical issues relating to both profitability and viability. A review of the financial statements for a number of accounting periods will be helpful in determining trends that would enable a CPA to compare the company's financial results with the costs required to comply with antipollution laws.

In order to assess whether a company can afford the costs of cleanup (particularly when that company claims it cannot), a CPA would need a crystal ball. In the absence of a crystal ball, the CPA should examine the company's budgets.

Management predicts the future by way of the budgeting process. Most enterprises that take the time to prepare budgets use them as tools for making financial and operating decisions. The range of budgets include operating budgets, capital budgets and cash flow budgets. A comprehensive operating and cash flow budget enables management to plan future operations and to decide how the company will pay for them. Access to past budgets, together with the corresponding historical results, allows the forensic accountant to interpret the proficiency of the company's budgeting process and to determine whether a company can or cannot afford the cleanup costs.

Mine Cleanup Case Study

In the 1990s the federal government filed suit against Mine Cleanup, a uranium mining company, for failure to clean up a former site. The mining company claimed it would be put out of business if it was required to pay the $30 million required to clean up the site. Mine Cleanup management was attempting to set aside the clean-up order.

A thorough review of the company's financial statements, operating budgets, long term forecasts, and cash flow budgets revealed that the company was unable to pay the costs in the short term, but that it was possible for the company to comply with the cleanup order over an extended period. A negotiated agreement was reached between the federal government and the company wherein the government essentially provided the long-term financing for the cleanup so that the cleanup operations could commence immediately.

Natural Resource Abuse

Laws with respect to natural resource abuse (over-fishing, hunting, logging, mining, and so on, as well as neglecting the endangered-species legislation) vary from jurisdiction to jurisdiction and generally apply to both noncommercial and commercial harvesting of animals, marine life, and endangered species. Accounting evidence has little relevance to noncommercial activities; thus the focus in this section is primarily on commercial activities involving the following three areas:

1. Fur trapping and fur dealers
2. Commercial fishing
3. Endangered species

Note that companies that are involved in these commercial activities need to be aware that conservation officers appear to have a much broader right of access to business premises than that available to law enforcement officers. Generally, the legislation allows the officers to search any aircraft, vehicle, vessel, camp, or office, without the requirement of a search warrant, if they believe that any fish or game has been killed or taken in contravention of the applicable state laws.

Fur Trapping and Fur Dealers. Fur trappers must be licensed to practice their trade in each state in which they operate. They are assigned maximum quotas for different kinds of wild life. They are generally required to have each pelt examined and registered, at which time a stamp is affixed to the inside of the pelt. The trapper is not required to submit written reports to the state; the next level in the distribution system does that.

The fur dealer obtains a license to purchase, receive, sell, or otherwise dispose of fur pelts. With a few limited exceptions (domestic animals, road kill, and so on) the fur dealer must ensure that the pelts being purchased have been examined and suitably stamped. Monthly reports are generally required from the fur dealer specifying:

1. The pelts purchased or received, including the name of the trapper or hunter from whom the fur dealer purchased or received the furs; the date on which such pelts were obtained; and the number and the kinds of animals, for example, beaver, mink, lynx, and otter.
2. The pelts sold or disposed of, including who the pelts were sold to by name, address, and license number; the date on which the pelts were sold, tanned or disposed of; and the number and kinds of animals.

The most common form of abuse is the handling of unauthorized pelts, which are purchased from a trapper or hunter, that are typically excluded from both of the monthly fur dealers' reports—that is, they are excluded from the report of pelts purchased, and from the report of pelts sold. These pelts typically bear no authorized stamp. The transactions often involve some financial consideration to the purchaser, for example, lower prices or secret commissions, which could be ascertained upon a review of the fur dealer's books and records. The unauthorized pelts are typically disposed of by being included in bundles of authorized fur pelts submitted to a fur auction outlet, or by being directly supplied to a tanning operation owned by the fur dealer.

Commercial Fishing. Commercial fishermen are generally licensed to work in designated regions within the United States and its waters, and are assigned maximum quotas by fish species and poundage. These fishermen are generally required to submit a monthly report that accumulates information on the port where the fish were landed, the weight of the catch by species, and the average price of fish sold.

Unlike the fur dealer, the commercial fisherman is not required to submit a report stating to whom the fish were sold.

The most common form of abuse involves the fisherman exceeding his quotas and failing to report the excesses in his monthly reporting. A review of the cash receipts, disbursements, and sales journals of the commercial fisherman should detect the abuse even though many purchases and sales are cash transactions that take place off the company's books. Because the reporting required is done by weight rather than by supplier or number of fish, it is necessary to reconcile the weight of fish caught to the weight of fish purchased by customers after allowing for wastage.

Endangered Species. In most jurisdictions, endangered species of fauna and flora are protected by laws that prohibit the killing, injuring, interfering with, taking, or attempting to do any of the above to any of the identified species of fauna or flora or their natural habitats.

Currently one of the major abuses is the exporting of certain endangered species of wild birds, particularly falcons, to other countries at an exorbitant profit to the perpetrators.

7.2.10 Economic Extortion

Economic extortion is a crime in which a financial benefit is sought or obtained through intimidation or persistent demands.

Some of the forms of crime described in this section of the Handbook could involve an element of economic extortion. For instance, bribes could be required in order to obtain a lucrative contract; an owner of a company could be squeezed out by one or more of its creditors for reasons other than insolvency; an employee could be forced to divulge an employer's trade secrets; or a company could be forced to pay a contractor to keep quiet about its environmental pollution problem. The common element in each of these situations is that the likely outcome of noncompliance with the extortionist's demands is perceived to be worse than the actual outcome of compliance.

Often, an extortionist's methods involve threats of physical violence, public disclosure of something that the victim would rather keep private, or financial ruin.

A Piece of the Action (Sport Megaplace) Case Study

In early 1994, Sport Megaplace was established as a state-approved organization to control the sale of lottery tickets in Megaplace and to apply the net proceeds from these sales to the development of amateur sports within Megaplace.

At that time the sale of lottery tickets included the sale of *Tinylotto* tickets, which was under the control of Mr. Johnson, and the sale of *Biglotto* tickets, which was under the control of Mr. Williams. These men were responsible for dividing Megaplace into wholesale distributorships so that both kinds of tickets could be sold regularly through wholesalers to retailers and then to the public.

However, Johnson and Williams only allowed others to obtain wholesale distributorships if they secretly agreed to pay 50 percent of the future profits to a holding company under the control of Johnson and Williams. The *silent-ownership* payments were structured as payments for management, consulting services and for office space.

The new distributors were led to believe that this arrangement was legitimate by the existence of a wholesale distributor agreement with Johnson and Williams' company, a reporting letter from a lawyer's office, a declaration of trust agreement, a power of attorney agreement, working papers from an accountant, banking resolutions and signature cards.

7.2.11 Customs Duty Fraud

Although customs laws vary from nation to nation, there are common threads and patterns of fraud that are inherent in transborder transactions. The following material describes typical customs fraud scenarios in Anyland.

The Customs Act applies to goods imported into Anyland. The Act categorizes imported goods by tariff schedules and prescribes rates of duty applicable to each item depending on its nature, the country of origin, and international treaty arrangements.

The duty payable to Anyland's Customs Service is a percentage (the duty rate) of the imported item's Value for Duty. Prior to January 1, 1998, the Customs Act based its determination of the Value for Duty amount on the fair market value of the goods at the time of export in the exporting country. In practice, this fair market value was usually the amount indicated on the commercial invoice. Customs officers did, however, have the option of disregarding the commercial invoice amount and determining a fair market value to be used for Value for Duty purposes using other information sources.

This fair market value determination for applying duty rates to imported goods did not comply with international trade agreements to which Anyland was a party. Thus, effective January 1, 1998, a revised procedure for determining the Value for Duty amount was introduced. The new basis, called the Transaction Value Method, specified the Value for Duty amount to be the price paid or payable to the exporter where the exporter and importer are dealing at arm's length. For imports between related parties, the onus is on the importer to prove that there was no influence on the commercial invoice price. In these situations, Value for Duty is determined on the following sequential bases:

1. Transaction value of identical goods
2. Transaction value of similar goods
3. Deductive value based on a gross profit reduction of the importer's selling price
4. Computed value

The abuse generally arises when the importer causes the Value for Duty of the imported product to be falsely understated, thereby reducing the amount of customs duty paid.

Importers abusing the customs regulations may vary in size of operation, ranging from small sole proprietors to large national distributors. The benefits from understating Value for Duty amounts can be enormous. In one case, the fine paid totaled $25,000,000, arising from a conviction of evading customs duties over a fifteen-year period. There was also a civil court claim for $105.2 million against the same company for unpaid duties on goods imported over a period of years. Even on a small scale, with duty rates ranging up to 30 percent or more, understating the Value for Duty amount may provide the importer with a 10-to-15 percent cost saving and a trade advantage over its competitors.

Because the Value for Duty amount generally is supported by both a commercial invoice and customs invoice prepared by the exporter, the duty and sales calculations rely on the integrity of the exporter's documentation. Many customs investigations have determined that the documents prepared by exporters understate the actual value at which the goods were sold.

Current customs practices continue to be conducive to fraud. Importers of legally importable goods are aware of the enormous volume of imports, the emphasis placed on illegal drug shipments, the shortage of customs officers, and the officers' inability to fully inspect all entries that provide a perceived window of opportunity to perpetrate fraud.

Investigation Issues

Red Flags. Customs investigations have uncovered various schemes to falsely reduce collectible duties. The presence of one or more of the following red flags may assist in identifying a customs under valuation.

1. *Apparent excess insurance:* Insurance coverage for the in-transit goods substantially exceeds the declared Value for Duty of the same goods.
2. *Competitor's complaints:* Competitor's complaints to customs or any other agency governing fair trade that it cannot match the importer's wholesale or retail prices.
3. *Poor quality documents:* The integrity of the exporter's documents may be suspect if any invoice is: printed on tissue paper, hand typed, not preprinted, or not prenumbered.
4. *Letters of credit or bank drafts:* Payments for the imported goods exceed the declared Value for Duty amount.
5. *Presence of blank invoices:* If Anyland customs invoices or export declarations, or the exporter's supplier invoices are known to exist at the importer's place of business and are found to be blank except for the exporter's authorization signature, the importer may be preparing such forms for presentation to Anyland's customs.
6. *Related exporter:* The importer and exporter are related parties and, therefore, do not deal at arm's length; there could be price collusion.
7. *A and B Commercial Invoices:* Total costs for the imported goods may be apportioned between two separate invoices (often having consecutive invoice numbers, or having the same invoice number with A and B suffixes), only one of which is submitted to customs for purpose of Value for Duty determination.
8. *Unreasonably high values allocated to nondutiable export costs:* The dutiable cost of product is artificially understated and the nondutiable cost of freight, for example, is overstated on the commercial and Anyland customs invoices.

Significance of the Accounting Evidence. After performing an overview, the forensic accountant can provide details for each entry and a summary schedule for all entries. This schedule quantifies the apparent Value for Duty shortage and calculates the apparent duty shortages, thereby determining the amount withheld.

In preparing this quantification, the forensic accountant assumes that documentation other than that used in the customs declaration in fact provides the *true* Value for Duty. The forensic accountant may need to obtain expert-witness evidence to substantiate this basis for valuation—perhaps a specialist from the Customs Service or from a lawyer.

In addition, in reviewing the importer's accounting books and records, the forensic accountant may be able to provide further support for the alleged undervaluation and may be helpful in refuting possible defense claims.

Testimony: Viva Voce Evidence. The forensic accountant may seek evidence from various other sources. Employees of the importer may be interviewed to provide evidence as to the inner workings of the importer and to settle issues of ownership or control of the importing company. A customs' broker may provide testimony that, if presented with the documents on which the forensic accountant's calculations were based, a higher Value for Duty would have been declared.

7.2.12 Health Care Fraud

There are a wide variety of health care frauds that have recently been the subject of media attention. Many such cases are outside the scope of this section—that is, they relate to fraud committed by individuals rather than by corporations. Health care fraud committed by corporations typically involves one of the following:

1. Violations of occupational health and safety laws (OSHA).
2. Marketing of drugs that have not been adequately tested or for which the test results have been falsified.

7.2.13 Possession of Property Obtained by Crime

This offence refers to either the actual possession of property obtained by a crime, or to the possession of proceeds from the disposal of property obtained by a crime.

When a business is suspected to be in possession of stolen inventory, an examination of the financial records should be able to establish whether this inventory had been legitimately purchased.

A reconciliation of the inventory purchased and sold needs to be performed and compared to the inventory on hand at both the beginning and end of the period in question: the end date is usually set shortly after the date that the stolen inventory was allegedly obtained. The purchases and sales should be ascertained from the company's purchases and sales records, and also from updated accounts payable and accounts receivable listings. If there is a positive variance, it could result from an accounting discrepancy, which would need to be examined further, or it could result from the possession of property obtained by crime.

If the purchases, on the accounting records, appear to be legitimate, then the integrity of the supplier invoices must be assessed. Often, stolen inventory can be made to appear legitimate through overstatements on supplier invoices.

Don't Fence Me In Case Study

Acme Industries was acting as a fence for stolen car parts. These parts were stolen by third parties and were sold by Acme to authorized car dealerships at prices considerably lower than normal wholesale prices. When Acme's premises were searched on December 8, 1998, parts valued at approximately $667,900 were seized.

Forensic accountants were retained to determine, by means of the available books of account and supporting documents, whether these parts were purchased legally or otherwise. Here are the steps followed to make the requested determination.

1. The accountant began by performing a period examination. The disbursement journal disclosed that a payment had been made to a firm of CPAs for services rendered to Acme. An interview with this firm revealed the existence of a draft set of financial statements for Acme, dated February 28, 1998. These financial statements, which were never issued in final form, disclosed inventory valued at $16,500, with a note stating, "no physical inventory taken; inventory estimated for accounts." The draft financial statements established the opening date of the time period. The closing date was determined by the date of search and seizure, December 8, 1998. The period March 1, 1998, to December 8, 1998, was, therefore, the period examined.
2. The accountant then updated the financial records of Acme to the date of search and seizure. This step disclosed purchases from various suppliers totaling $886,167. A similar updating of the sales of Acme resulted in a sales figure of $1,007,815.
3. To calculate the book value of inventory, the accountant created a schedule, identified as *Apparent Inventory of Acme as of December 8, 1998.* It set out the total value of the goods available for sale of $902,667 (opening inventory of $16,500 plus the purchases made, during the period, of $886,167).

   The schedule set out the updated sales figure and a gross profit margin (sales minus cost of sales divided by sales) ranging from 10-to-30 percent. By deducting the gross profit margin, an apparent cost of goods sold was calculated, ranging from a high of $907,000 at the 10 percent level to a low of $705,470 at the 30 percent level. A comparison of the apparent cost of goods sold to the value of goods available for sale showed that there should have been no inventory as of December 8, 1998 at a 10 percent gross margin. At a 30 percent gross margin, the value of inventory at December 8 would have been $197,197.
4. To perform a valuation of the parts seized, the accountant compared the goods seized to the inventory on hand calculated at the 10 percent gross margin level, indicating an excess quantity of physical parts on hand of approximately $672,200. When a gross profit margin of 30 percent was applied, the excess on hand was approximately $470,000. Based on the above procedures, Acme had in its possession an excess quantity of parts ranging in value from $470,000 to $672,200.

Interviews with three suppliers indicated that the invoices used in the calculation of purchases between March 1 and December 8, 1998 had been inflated or padded so that the invoiced value of goods purchased by Acme was greater than the actual value of the goods received. The padded portion of the payments Acme made to its suppliers were paid to the wife of Acme's owner in cash.

Padding the supplier's invoices made the stolen goods on hand harder to detect or easier to explain away, or both. The inflated purchase prices also allowed cash to be removed from Acme, tax free, under the guise of an expense. The payments to suppliers were converted into cash with the excess (padded) portion of the invoiced price being returned to the owner's wife as cash.

This disclosure made it necessary to revise the calculated value of inventory as of December 8, 1998, to reflect the alleged nonpurchases in Acme's dealings with the three suppliers who were padding their invoices. These alleged nonpurchases totaled some $263,000, thereby increasing the value of the excess quantity of parts in the possession of Acme to a figure between $735,000 and $935,000. These findings not only placed the onus on the owner of Acme to explain the source of the excess quantity of parts seized but also disclosed the existence of a fraudulent scheme involving the three suppliers.

7.2.14 Coupon Redemption Fraud

Coupon redemption fraud involves the fraudulent collection and conversion of coupons designed to promote various kinds of merchandise. For example, a newspaper coupon for a box of cereal may require the purchaser to present it at a supermarket to receive twenty-five cents off the purchase price of the cereal. Normally, the manufacturer reimburses the supermarket for the discount it paid plus a token fee, perhaps several cents, to cover the cost of processing the coupon and returning it to the manufacturer.

Unscrupulous grocery and supermarket owners will collect coupons, in some cases from an intermediary, and redeem them as though merchandise has been purchased from them, when in fact, it has not been. Although the individual amounts can be small, the volume in most consumables can make it profitable for stores to engage in these schemes.

7.3 Prevention of Commercial Crime

Four forces can operate to reduce commercial crime:

1. Increased awareness—that is, decreasing the likelihood that a victim will be "taken."
2. Formal deterrence—that is, the fear of formal, officially imposed sanctions (conviction and punishment by the government).
3. Informal deterrence—that is, the fear of informally imposed sanctions, such as the loss of respectability or a career.
4. Ethics—that is, the internalization of values that discourage violations of legal codes.

7.3.1 Increased Awareness

Increased awareness is achieved through education and by experience. However, experience can be a costly way to increase awareness. With increased awareness, the investor, customer, competitor, and general public are more likely to closely scrutinize a situation and ask questions that would raise alarm bells and prevent them from suffering a loss. For instance:

- Investors should be wary of schemes pitching high rates of return in a short time.
- Investors also should be wary of schemes with foreign intrigue.
- Investors should thoroughly examine franchise opportunities before any funds are invested. Brochures and marketing pitches should be viewed with skepticism, particularly in the case of new or unconventional franchisers. Detailed financial information, including costs and profit margins of the franchiser for any goods and services they are contracting to provide, should be reviewed to determine the motives of the franchiser.
- Investors should ask stock promoters a series of questions about the stock the promoter is pushing to determine the extent to which that promoter is tied to the stock.

7.3.2 Formal Deterrence

A crime control strategy has little chance of success unless offenders are punished. However, formal levels of current enforcement are, by all measures, extremely low. One novel approach is enforced self-regulation. Under this idea, the government would compel each company to write unique rules for itself or its employees. A governmental agency would monitor compliance. Two examples of successes in the noncriminal area are the Federal Aviation Administration, which monitors self-regulation for the U.S. airline industry, and the Federal Trade Commission, which monitors rules that the U.S. advertising industry has largely set for itself.

However, there are problems with self-regulation, and the industries that attempt to regulate themselves have spotty records at best. In one study of the 320,000 physicians in the United States, an average of only seventy-two medical licenses per year were revoked.

It may be that increased enforcement can only come at the expense of a complete and total revision of the criminal justice system. Many commercial criminals have little fear of detection because of the constant barrage of information that demonstrates the police and courts simply cannot keep up with the pace of criminal offenses. Until potential offenders have the perception that they will be caught and punished, we should not expect a reversal of this crime trend.

However, many researchers believe there are better deterrents to commercial crime than incarceration of the individuals who are directly involved. They argue that the most effective deterrents are:

- Monetary penalties
- Adverse publicity

The following remedial steps could be adopted to deal with commercial crime:

1. Strengthen consent agreements and decrees (under which companies do not admit that what they were doing was wrong, but agree to stop doing it) to provide substantial remedies for violations of the agreement and to include systematic follow-ups.
2. Increase fine ceilings, assessing fines according to the nature of the violation and in proportion to the company's annual sales.
3. Enact stiff criminal penalties for violations of health and safety or environmental regulations that recklessly endanger the public or employees.
4. Introduce stronger statutes to prohibit companies that previously had violated federal laws from receiving federal contracts.
5. Promote mandatory publicity for corporate civil and criminal violations.
6. Increase more extensive use of imprisonment with longer sentences. Replace community service with incarceration, except for unusual circumstances.
7. Prevent convicted corporate offenders from being indemnified by their companies.
8. Prohibit for three years management officials convicted of criminally violating corporate responsibilities from assuming similar management positions in their company or others.
9. Make directors liable, but not criminally, for being derelict in their duty to prevent illegal corporate actions.
10. Enact a new commercial bribery statute to help prosecute corporate executives who receive kickbacks from their customers or suppliers.

7.3.3 Informal Deterrence

Most commercial criminals, compared to more traditional offenders, perceive the informal sanctions of the loss of career and prestige to be a greater deterrent. They are, therefore, theoretically more deterred from misbehaving by those consequences than by incarceration.

For example, a bank president, who was told he was about to be indicted, spent most of his time asking whether the charges were going to be made public. When told that indeed the charges would be public, the banker, promptly committed suicide.

Informal sanctions often exist without formal sanctions. The imposition of formal sanctions, however, will usually lead to additional informal sanctions.

7.3.4 Ethics

Behaviorists generally conclude that one of the single most important factors influencing group behavior is the attitude of management, who—in many reported instances—have been claimed by employees to have exerted pressure on them to engage in unethical behavior.

One prime example is the famous Equity Funding Case, which occurred in the early 1970s. It was uncovered when a disgruntled former employee went to the authorities. For nearly ten years, the Equity Funding Corporation falsified more than 56,000 life insurance policies and overstated their assets by $120 million. It was estimated that fifty to 75 employees, who managed to keep the scheme a secret for several years, were involved. The trustee appointed to sort out the massive fraud, Robert Loeffler, said, "Of almost equal importance was the surprising ability of the originators of the fraud to recruit new participants over the years."

Teaching people that certain behaviors are illegal and therefore inappropriate is uncomplicated and extremely effective in reducing crime. Moral education that discourages illegal behavior, from the top to the bottom of an organization, must be continuous. Simply put, people must be informed as to what behavior is acceptable and what is not so that they can alter their actions appropriately.

Computer Crime and
Computer Criminals

CHAPTER 8:

Computer Crime and Computer Criminals

CHAPTER 8:

Computer Crime and Computer Criminals

8.1 OVERVIEW

The advent of the computer has made certain kinds of crimes more efficient, harder to detect, and very difficult to prosecute. Add to this the fact that, in a global corporation, computers are likely to be operated all over the world; even where a company operates in only one country, access to the Internet connects the company to the world.

A computer-related crime is simply one in which a computer is used either to commit a crime, or as the target of a crime. Crimes committed using computers may include: embezzlement, larceny (theft of property and proprietary information), fraud, forgery and counterfeiting. Crimes committed targeting computers may include sabotage, vandalism, electronic burglary, wiretapping, and the gaining of illegal access, either by impersonating an authorized user or by exceeding one's authority.

Some people incorrectly assume that in order to commit a computer crime, which carries with it the risk of a substantial prison sentence, a person must be a computer scientist, information technology specialist or programming genius. However, anyone with access, or who can gain access, to a computer managing assets or confidential information is in a position to commit the crime.

Until a few years ago, computer crime was something most people considered to be in the realm of science fiction, or one that involved cyber-wizards in lab coats doing incomprehensible things to giant computers. Today, nothing could be further from the truth. Surveys show losses from computer crimes in the billions of dollars. The high valuation that the investment community places on companies providing computer security solutions is testimony to the importance that computer security plays in the modern organization.

8.1.1 Security

Assuring security for a computer system is no different than having appropriate security for manual accounting files. Because of the disparity in technology, each system requires its own particular tools and methods to implement security, but the objective is the same: to achieve a reasonable and cost-effective control environment in which an unauthorized act is likely to be detected.

Of course, that technology has changed radically over the last decade, as companies have moved from large central systems to interconnected local and wide area networks (LANs and WANs), and since the Internet has made email and communications a part of almost everyone's lives. Security measures from years past that were accomplished by locking up the room containing the mainframe don't work today. One central machine has been replaced by hundreds of PCs (each probably exceeding the power of that old mainframe in many ways) connected into internal networks, and likely interconnected to the outside world as well. Terms such as *firewalls* (programs designed to prevent invasion of a system by an outsider), which had no real applicability to the world of computers as little as five years ago, are now essential requirements for any reasonably managed corporate or government computer operation.

8.1.2 Evolution of Computer Crime

In looking at computer crimes, it's important to remember that computers are just machines that carry out instructions programmed into them. When a crime involves a computer, it isn't the computer suddenly deciding to become a criminal, but the person manipulating the program or using the computer to perpetrate an act that has been defined in law as being criminal. Computers are an instrument of the crime, in the same sense that a phone or fax machine can facilitate the commission of an insider trading offense. And while certain kinds of crime would not be possible without a computer–for example, planting a computer virus, others are new versions of old crimes that are facilitated by modern computer technology. As technology advances, those with a criminal mindset will, inevitably, continue to look for new ways to exploit the computer for their own ends.

For example, consider the theft of a new computer chip design. Printed out, the details of the design might require a dozen thick notebooks and a large roll of detailed circuit diagrams. That same information in computer form would easily fit on a small tape cassette, smaller than the common audiocassettes used for music. Or, in minutes, the information could be transmitted via the Internet, either as a file or as an attachment to one or more email messages.

Most experts agree that computer crime is a growing problem, and that the tools to prevent it are evolving, but so are new ways of committing those crimes. Feeling confident that your systems are 100 percent secure is never a good idea, but given the speed of computer evolution, today, it is downright dangerous!

This chapter should provide you with an understanding of computer crime, how it has evolved, and the ways that computer criminals are likely to attack organizations like yours.

8.2 COMPUTER-RELATED CRIMES

In today's organizations, virtually every asset, from money to proprietary and confidential information, is likely to be recorded on some computer's hard drive, on a computer tape or on a disk. Every day trillions of dollars are transferred between bank accounts relying on computerized records. Millions of individuals essentially never see the inside of a bank. Their pay is deposited directly into their accounts, and when they need cash, they head for the nearest automatic teller machine (ATM). Yet money may not be the most valuable commodity on the computer.

8.2.1 Intellectual Property

Intellectual property, which can range from business plans to trade secrets, can have immense value. There are unique differences between stealing information and stealing almost anything else. If $100 is stolen from you, the thief has deprived you of your money.

Similarly, if your car is stolen, the thief has it and you don't. With information, however, particularly information stored on a computer, a thief can steal the information and you can still have it. If the thief is a really good crook, your information can be stolen without you ever knowing that an incident has taken place. So computers can be used to facilitate the theft of money (for example, by manipulating banking or accounting records), the theft of goods (by manipulating inventory, shipping records or receivables records) or information (usually by copying it). This category includes computer-based implementations of traditional crimes (theft, insider trading, and so on) and of newly defined crimes such as economic espionage in which company secrets are stolen for the benefit of another organization, or computer intrusion, which criminalizes the unauthorized access into another organization's computers.

8.2.2 Computer Hardware

Another class of computer crime attempts to target the computers themselves. If a perpetrator can put a computer virus into your computer, the virus can cause a huge disruption of your business when it is triggered to destroy data (particularly if you haven't been backing up that data regularly). In some cases, criminals may take more direct action to damage your computer. These attack profiles are sometimes referred to as *denial of service* attacks, because they are designed to deprive the rightful users of the use of their systems' resources.

8.2.3 Computer Crimes and the Law

Whether a target of an attack is the computer itself or the information residing in the computer, the attempt may well be a crime. But what if it isn't?

To be a crime, there has to be a law that declares a particular course of action to be a criminal act. Until the passage of specific computer crime laws over the past twenty years, prosecutors had to find ways to apply traditional laws, such as, wire fraud or mail fraud, to high-tech crimes. And it is important to remember that laws only apply within the state or country in which they are promulgated. Because the Internet can be accessed from anywhere in the world, perpetrators can carry out crimes from anywhere, including from countries that have weak computer crime laws, or from which extradition is unlikely. Some laws specifically require the victims to show that they had safeguarded the information stolen or provided notification that the information was not in the public domain.

Unfortunately, in our society, there are too few law enforcement and prosecution personnel who are specialists in computer crime investigation. There are very specific procedures that must be followed in handling and analyzing computer files and equipment if the evidence of the offense is to be admissible in a court of law. Failure to do so may cause a prosecution to fail. Corporations should be aware that attempts of their in-house technical or investigative personnel to examine computers involved in an offense, however well intentioned may result in evidence being rendered inadmissible. Once a crime occurs, a court is going to apply the rules of evidence to determine whether any actions taken could have modified the evidence or otherwise damaged its credibility.

8.3 A Brief History of Computer Crime

No one knows who the first computer criminal was. However, computer-related crimes certainly have been around since the early 1970s. Throughout the rest of that decade, computer crimes tended to focus on the manipulation of computer records to obtain money. In the 1980s, we began to see cases in which the target of the crime was the information on the computer. Insider trading was facilitated by the relative anonymity with which information could be accessed in many systems.

In one of the largest early cases, an insurance company took advantage of its accounting firm's computer naiveté to perpetrate a huge fraud. The insurer created thousands of bogus policies, which it could identify through special policy numbers. When the auditors, as part of random checks, wanted to see some of these nonexistent policies, they were told the policies would be available the next day. That evening, the perpetrators busily created the appropriate documentation to prove the validity of the policies. Millions of dollars were funneled out of the company through this scheme. This case marked the period when auditors learned that it was vital to include computer systems in their audit plans.

In another noteworthy case, the chief teller of a bank located in Brooklyn, NY, devised a plan to manipulate dormant accounts using the bank's new computer system. He discovered that he could move money in and out of those inactive accounts simply by using his supervisor's key. He *withdrew* several hundred thousand dollars. Even though the manipulations all showed up on accounting reports, there were so many thousands of irregularities as a result of the complex new systems that the internal auditors were not able to keep up with the volume, and ignored what they considered low-priority items, like dormant account transactions. Unfortunately for the perpetrator, he was a dedicated (but spectacularly unsuccessful) horse-player. When the Attorney General of New York State conducted a raid on his bookmaker, the volume of his gambling was discovered, and the source of his funds uncovered. He was convicted of theft and imprisoned.

In another case, in California, a young man discovered that the phone company had installed a system that permitted their employees to order equipment to be delivered to job sites using a push-button phone. He obtained the requisite code numbers from manuals recovered from the phone company's trash. Using the codes, he ordered the computer to arrange the delivery of equipment to downtown manholes. He then collected the valuable materials with his own truck, and eventually sold the valuable equipment to foreign phone companies. His scheme was discovered when he refused to give his truck driver a raise, and the driver turned him in. It was shown that he had stolen about $1.1 million in equipment. He was tried, convicted, and after a short 90-day stay in jail, promptly established a business as a consultant to attorneys who defended computer criminals. His ads proudly proclaimed that he had "actual courtroom experience."

Today, computer crime has progressed from crimes committed by individuals against individuals and companies to a topic of great concern to governments: *information warfare* has emerged as a real threat to national infrastructures.

8.4 Computer Crime Today

Computer crime is in the news. Whether it is the arrest of the creator of a damaging computer virus or a person using computers to sell child pornography, the media has realized that our society has become worried about technology failures. This media attention has had an unintended effect that can be a problem.

If you were to believe the media, hackers are the number one cause of computer crime problems. In fact, however, the major problem is computer-facilitated crime committed by employees and others who have been granted access to a system. Because the common perception of threats is one of the key inputs people use for deciding how to spend their security dollars, this misperception may lead to an inappropriate distribution of resources, so that risk does not match security measures. Today many companies are realizing that this may well be the case.

The problem of preventing computer crime is no different than that of preventing any other crime against a business. After all, crimes were committed against business long before computers. Accountants worked to discourage these crimes by requiring separation of duties between people handling cash or other assets and those making the entries in the books of the company concerning the assets. By dividing access to assets and the records of those assets, the theory was that two or more people would have to conspire to carry out a fraud, thus increasing the likelihood of detection.

Along with separation of duties, accountants have traditionally depended on the paper trail of records that document transactions. This paper trail required that all transactions be entered into journals that would be backed up by source documents, such as invoices, purchase orders, receiving reports, canceled checks, sales receipts and vendor invoices.

Of course, in spite of the best efforts of the accountants, fraud did occur. Accounting systems are neither foolproof nor fraud proof. Determined criminals could still find ways to circumvent or override controls.

Computers haven't really changed anything. A crook is still a crook. Fraud, theft and embezzlement are still possible in the age of computers. Indeed, some argue that crime has become more likely, as traditional paper trails are replaced by computerized trails, which are not as easily verified by traditional methods. The speed of processing took precedence over effective control, according to some writers. CPAs should determine how and what to do to validate the information stored in computer systems. And that has become more difficult as computer architectures have evolved from central mainframe computers to networks of hundreds or even thousands of PCs and file servers distributed throughout the company.

As stated earlier, surveys, including those conducted by the Federal Bureau of Investigation, the Computer Security Institute, and the American Society for Industrial Security, show that computer crime is responsible for billions of dollars of loss each year. Many of these surveys indicate that the average loss in a computer crime is higher than in noncomputer-based crimes. It is often more difficult to prosecute a computer crime than a traditional crime. Evidence on a computer is very difficult to connect to an individual because computer data can be manipulated; therefore, providing proof not only that the crime occurred but also how it was accomplished can be a complex process. Part of the problem is that there are a limited number of police and prosecutors who are trained in the investigation and prosecution of computer crime.

In fact, new opportunities for theft, fraud and embezzlement have been created by computer technology. Accounting records, once kept under lock and key in the accounting department, are now stored on computers that can be accessed remotely. Not only are the systems available to authorized users (employees who have a job-related requirement to access and use the accounting system) but also by data entry clerks, computer operators, systems analysts and programmers. If the computer's access control security system is not set correctly, unauthorized employees or even outsiders could gain access to the system. With the proper skills and a criminal inclination, systems can be manipulated, and programs changed to eliminate records of the fraud.

8.4.1 Classification of Computer Fraud

Generally, there is no accepted *chart-of-accounts* for computer fraud. If there were, it would constantly be changing. But certain computer-fraud activities that could affect a business' chart-of-accounts should be recognized: manipulating computer inputs, manipulating programs and tampering with outputs.

Manipulating Computer Inputs

One of the most frequent bases of computer crime involves the falsification of computer inputs. Those inputs may involve putting false transactions into the system, modifying actual transactions, or in some schemes, not putting information into the system.

From an accounting standpoint, the main reasons for manipulating inputs are to overstate or understate revenues, assets, expenses and liabilities. The objective of the perpetrator determines the manipulation necessary. Sometimes the objective is to provide false data to managers, stockholders, creditors or government agencies. Sometimes the manipulation is part of an embezzlement, for example, entering false invoices into an accounts payable system. There can be little question that the manipulation of data is the most common form of computer-related fraud.

Input fraud should be among the easiest to detect and prevent with effective supervision and controls. These include:

- Separation of duties
- Audit trails
- Control totals and access controls (both those that limit access to data entry screens and those that place limits on values that can be entered)

Manipulating Programs

Another major class of computer crime involves altering the instructions that computers use to manipulate input files and databases. These can range from schemes in which programs are designed to process fraudulent entries without making audit trail entries, to those featuring deliberate miscalculations (for example, to shortchange depositors of a bank of fractions of a cent of interest, which can be accumulated and stolen).

Tampering with Outputs

Yet another category of computer fraud involves tampering with the results of computer activity: reports and files. This category includes theft of confidential or proprietary information (customer lists, research and design [R&D] results, company business plans, employee information, secret formulas, and so on). According to the previously mentioned surveys these intellectual property thefts are apparently escalating as competition increases globally. Computers have undoubtedly facilitated the thefts, because they have provided the capability for fast copying of huge databases, and at the same time provided, through data communications, the capability for moving the copied data globally at tremendous speeds. Intellectual property theft by computer is a unique crime: someone can steal your data, but it's still where it originally was, and there may be no record of the crime.

8.4.2 The Most Common Computer Crimes

With all of the hype concerning hackers, you would think they represent the major threat of computer crime, but nothing could be further from the truth. Regardless of the evolution of computer technology, the manipulation of inputs and outputs is still the most common form of computer-related crime.

Computers are frequently manipulated to get to assets, the most popular of which are either cash or information that can be converted to cash, or both. In terms of cash, input is frequently manipulated through submission of falsified documents, such as invoices from vendors, suppliers or contractors; claims for government benefits; refund or credit claims; or fraud involving payroll or expenses. The phony claims can involve anyone from clerks to senior executives, although employees in either the claims approval or accounting functions are most often involved. From an accounting viewpoint, the false claim is a fake debit to an expense so that a corresponding credit can be posted to the cash account to cover the issuance of a check or funds transfer.

Executive Computer Crimes

In the higher levels of an organization, the nature of fraud changes. Rather than simply grabbing cash, fraud may be designed to overstate profits by fabricating data such as sales (which are simply overstated or which are booked before the transaction is really completed), or by understating expenses (either by simple reduction of the numbers or in improper deferral to a later accounting period). There is a nearly infinite range of variations on these themes, based on the ingenuity of the perpetrators. For example, profits may be overstated by increasing ending inventory of manufactured goods or merchandise held for sale. That results in understatement of the cost of goods sold and raises the net profits.

Manipulation of operating results is probably more highly motivated today than ever before. With increasing market volatility as well as an insistence on continuous growth and on beating analyst expectations every quarter, managers may turn to manipulation to borrow time in order to turn around what they may believe to be temporary problems. With so much of their personal wealth tied up in company stock, there is a tremendous motivation to keep the numbers where the market perceives they should be. Or it may be done to make the company a more attractive merger or acquisition target, with the assumption that in the course of the merger the falsification would be overlooked or attributed to some undefined error. Or it may be done for personal greed; in some companies, the executive compensation plan is directly tied to reported results.

8.5 Computer Criminal Profiles

Who commits computer crime? It would be useful to have a profile of the offender so that we could perhaps predict who will commit the crimes.

8.5.1 Predictions

In the 1980s, criminologists, who focused their attention on white-collar crime, argued that the perpetrators tended to be trusted employees with unresolvable personal problems, usually financial in nature. These included indebtedness as a result of illness in the family, or problems with alcohol, narcotics, gambling, expensive tastes, or sexual pursuits (according to the police, the *three Bs*: booze, babes and bets).

At about the same time, various studies provided a profile of the computer criminal. In this profile the culprit—

1. Is male, white, and between19 and 30 years of age.
2. Has no prior criminal record.
3. Identifies with technology more than with the employer's business.
4. Is bright, creative, energetic, willing to accept challenges, and highly motivated.
5. Is employed in the field of either information processing or accounting.
6. Feels a desperate need for money because of personal problems.
7. Feels exploited by his or her employer and wants to get even. The culprit feels that promotions, salary increases, bonuses, stock options, and so on, are not fairly distributed. Others have gotten more than they deserve through various forms of favoritism.
8. Does not intend to hurt people, just the employer, who is perceived of as cold, indifferent, uncaring and exploitive.
9. Does not have a self-image as a criminal.
10. Believes that actions against *the establishment* are justified for political or social reasons.
11. Perceives beating the system as a challenge worthy of his or her efforts.

In addition, there are four frequently cited characteristics that are symptoms of trouble:

1. *High living:* Not too long ago, eyebrows were raised at the programmer who showed up in the company parking lot in a new Mercedes convertible. However, in the turn of the century marketplace, programmers who have been through one or two initial public offerings (IPOs) can easily afford any car they want. Nonetheless, a discrepancy between life-style and income must be regarded as suspicious.
2. *Ultradedication to the job:* The bookkeeper or computer programmer who never takes a vacation is either very dedicated (increasingly less likely in today's business environment) or afraid that some scheme would come to light if he or she were not around to control things.
3. *Aging:* As some people age, they grow increasingly resentful of perceived wrongs; for example, the awarding of increased salaries and stock to younger employees. Therefore, they may feel justified in making a big score if they think they can get away with it.

4. *Chronic Lateness*: The common wisdom held that people who were constantly late with their work were late because they were trying to fabricate or cover up something they were doing.

In today's environment, how valid are these assumptions? We do know that most perpetrators who are caught committing computer crimes are male. They also tend to be young. But there are not a lot of reliable indicators in the above lists that provide any kind of predictive ability. Does this mean that the perpetration of computer manipulations is unpredictable?

Certainly, there is no simple test that will detect whether a person, who has never committed a crime in the past, will or will not commit one in the future, given the proper circumstances and motivations. However, a review of cases over the past few years reveals one interesting phenomenon: those who committed these offenses often had problems with former employers who were glad to be rid of them. Companies that do not perform background checks that include contacting former employers and checking for falsification on employment applications are the fraudster's friend. The perpetrators can ignore their pasts and start anew at a company that appears to have weak security. Certainly, former employers can lie about an employee or refuse to give any reference beyond confirmation of employment, but a good background check should pick up at least some potential problem employees.

Three other things to say about perpetrators are important. First, an offender does not have to be a computer genius to pull off a major fraud. Anyone who can gain access to a system, either because he or she is authorized to use it, or because the security controls are weak, can potentially manipulate that system for personal advantage. Even if they cannot directly access the computer, if they can fake the data, they can manipulate it.

Second, it is easy to limit consideration of risk to employees. Many companies today, particularly in high-tech industries, make considerable use of temporary employees and independent contractors. All too often, because they are not carried on the books as employees, they are not subject to the same background checks and security measures. It should be clear that computers don't care if they are manipulated by employees or independent contractors. If a person has access, they should be subject to the same controls as regular employees.

Finally, there are offenders you will never meet, who will never meet you, but who may cause you great difficulties. These are the virus writers and virus distributors who develop and spread them simply because they can.

8.5.2 Reasons for Committing Computer Crimes

Criminologists, in looking at why crimes are committed, often use a four-element model, sometimes called Motivation, Opportunity, Means, and Methods, (MOMM).

Motivation represents the reason why one is willing to commit a crime. Motivation can be related to both personal (or internal) conditions and external conditions. Personal motivation factors include:

- *Economic Motivators:* Economically motivated perpetrators act to fulfill the need or desire for financial gain, for money or for other assets (or information) that can be turned into money.
- *Egocentric Motivators*: Egocentric perpetrators have a need to show off their talents in committing what may be perceived by others as a complex crime. Money or other assets are sometimes part of the crime, but frequently they are not the underlying motivation. Certainly, assets symbolize a measure of the success of the venture, which is important in demonstrating the prowess and ingenuity of the criminal. Many hackers fall into this category. But for many others, their downfall is the need to brag about their exploits and thus gain favor in the eyes of their peer group.
- *Ideological Motivators*: Ideologically motivated perpetrators feel compelled to seek revenge against someone or something they perceive as oppressing or exploiting either them personally or other individuals possibly unknown to them. Terrorist bombings of computer centers is an extreme example of this mindset. Sabotage against systems by disgruntled employees or exemployees is a frequently encountered motivator.
- *Psychotic Motivators*: Psychotic perpetrators (that is, people suffering from mental disease) may view the company through a delusional state of mind that does one or more of the following: distorts reality, validates feelings of grandeur or of persecution, or exaggerates hatred or fear of the organization or of particular people in the organization (often direct superiors) to the extent that they may commit extreme actions against their perceived enemies to relieve their anxieties. One way of acting out these feelings is exemplified by the person who shows up at the office with a gun and kills those he or she believes are "out to get them." Another way this kind of troubled individual may lash out at these imaginary adversaries is to attack the computer systems that may be perceived as facilitating the work of supposed enemies. The subject of workplace violence is an important one, but is outside the scope of this Handbook.

Environmental Motivators

Environmental motivators are those conditions in the environment of the company (or sometimes of society in general) that are claimed as motivators. But no external motivator forces anyone to commit a crime. It would be fair to say that environmental motivators may aggravate personal motives. These include the work environment, reward systems, levels of interpersonal trust, corporate ethics, stress and weaknesses in internal controls, or security systems that may make a person believe that they can get away with a crime.

It was indicated earlier that there are no guaranteed ways of spotting a computer criminal any more than any other kind of criminal, and that people commit offenses for many different reasons. Does this mean that there's nothing we can do to prevent computer crime? Nothing could be further from the truth. We may not know specifically who will commit a crime, but we know that given the right circumstances, someone is likely to try. In the next section, we will look at the things a business can do to reduce the chance that it will be victimized by a computer criminal.

8.6 CONTROLS FOR PREVENTING AND DETECTING COMPUTER CRIME

It would be nice to assume that everyone associated with a business is honest. Certainly, it would eliminate the need for controls to prevent crime. Of course, that assumption is not viable. People will commit crimes for many reasons, some of which are rational, others of which may make no sense to the observer. The larger the organization, the more likely it is that someone is out to commit a crime. Managers who subscribe to this belief are not necessarily paranoid. In fact, most managers can name their disgruntled employees.

There are those who will steal under the best of employment circumstances. Others would not steal even if they were unfavored employees of Ebenezer Scrooge (*before* the events in *A Christmas Carol*, of course.)

8.6.1 Internal Control and Security Systems

Internal control and security systems are designed on the basis of past experience both in the company in which they are installed and in other companies. The challenge here is to build in enough controls to discourage and catch criminal behavior without breaking the bank in costs or going overboard on security. Companies that have been victimized often react by increasing controls to the point at which the controls can become oppressive and actually interfere with company operations. While rational companies set up rules to define acceptable and unacceptable behavior, too many constraints make people feel oppressed, distrusted, and under constant surveillance.

Our society is based on freedoms and rights. We highly value our freedoms of speech, religion and assembly, but these freedoms are not absolute. We can speak our minds, but we cannot freely slander or libel another individual. We cannot, as one famous jurist put it, feel free to yell "FIRE" in a crowded theatre. We cannot trade on inside information (unless we like prison food) or release secret company information (unless we like having the opportunity to spend time as a defendant in both the criminal and civil courts.)

Well-designed controls should provide similar checks and balances. We need to consider the risks, threats, and other vulnerabilities in today's marketplace and technological environment, while simultaneously taking into account our responsibilities to employees, the value of their contributions, and their need for satisfaction in the workplace, including the provision of a work environment that encourages outstanding performance, profitability, and efficiency.

A competent systems analyst or information security specialist can design layer upon layer of controls. But controls in excess of those required by the nature of the risks are not cost-effective and can place undue burdens both on those who must work under them and those who must monitor and control them. So a company's requirement for an effective internal-control environment does not represent a justification for a siege mentality or the construction of an impregnable fortress. Done effectively, the development of internal controls is a matter of proper balance and equilibrium, not of the implementation of paranoia.

Looking at the potential for theft and fraud and the actions available to prevent crime, brings forth several conclusions:

- Most prevention efforts concentrate or focus on building more accounting and access controls or physical security controls.
- It is vital to recognize that there are limits to technological and procedural controls. Given the speed with which computer and data communications technology evolves and the complexity of modern systems, it is difficult for improvements in protection and detection mechanisms to keep pace.
- It is also important for companies to recognize that improvements in the working environment, including a positive ethical climate and strong interpersonal trust, help to discourage criminal thinking and behavior and, as a result, are a part of the control environment. Some factors in the business environment are likely to encourage computer crime. Other factors discourage crime. Clearly, we want to minimize the criminal behavioral motivators, and maximize the noncriminal behavioral motivators.

8.6.2 Factors That Encourage Computer Crime

The factors that enhance the probability that a company will be the target of theft, fraud, embezzlement and corruption, including computer crime, can be either motivational (related to the corporate reward system and company policies) or personal (relating to the personal character of a particular employee).

The following are motivational factors that encourage computer crime:

- Inadequate rewards including pay, fringe benefits, stock and stock options, bonuses, incentives, perquisites, job security, meaningful work and promotional opportunities.
- Inadequate management controls, including failure to communicate expected standards of job-related performance or on-the-job behavior, and ambiguity in relationship to work roles, relationships, responsibilities, and areas of accountability.
- Inadequate reinforcement and performance feedback mechanisms, including lack of recognition for good work, loyalty, longevity and effort; lack of meaningful recognition for outstanding performance; delayed or nonexistent feedback on performance inadequacies or unacceptable on-the-job behavior.
- Failure to offer counseling when performance or behavior falls below acceptable levels.
- Acceptance of mediocre performance as the standard.
- Inadequate support and lack of resources to meet standards, such as not providing authority to hire sufficient personnel to meet requirements for quality, quantity, and timeliness of work produced.
- Inadequate operational reviews, audits, inspections, and follow-throughs to assure compliance with company policies, priorities, procedures, and government regulations.
- Condonation of inappropriate ethical norms or inappropriate behavior.
- Failure to control hostility generated by promotion or destructive competitiveness among departments, offices, or personnel.
- Failure to control bias or unfairness in selection, promotion, compensation and appraisal.

The following are personal or personnel-based encouragements of computer crime:

- Inadequate standards of recruitment and selection.
- Inadequate orientation and training on security matters and on sanctions for violating security rules.
- Unresolved personal financial problems.
- Unresolved problems relating to personal status.
- Failure to screen and background check personnel before appointing to sensitive positions. This includes verification of prior employment, verification of educational qualifications, verification of financial stability, and examination of character.
- Inadequate control of the level of job-related stress and anxiety.

8.6.3 Factors That Discourage Computer Crime

Computer crime can be discouraged through measures that are designed not only to prevent crime but also to detect attempts to engage in computer crimes. The recommended prevention measures are—

1. Internal accounting controls. These are the traditional measures that discourage crime, and they are as important in an automated environment as in a manual-processing environment. These include:
   - Separation and rotation of duties. Remember that as personnel change jobs, it is vital to update the list of computer applications that they can access, so that their access at any given time matches their current job requirements.
   - Periodic internal audits, surprise inspections and computer security reviews.
   - Absolute insistence that control policies and procedures be documented in writing.
   - Establishment of dual signature authorities, dollar authorization limits, expiration dates for signature authorizations, and check amount limits. These authorities also should be examined on both a routine and surprise basis.
   - Offline controls and limits, including batch controls and hash totals.
2. Computer Access Controls. These controls may include:
   - Authentication and identification controls, including keys or smartcards, passwords, biometrics, callback systems, one-time passwords, time and day constrained access, and periodic code and password changes.
   - Compartmentalization, also known as *need to know*.
   - Use of encryption to protect data while stored or in transit.
3. Use of firewalls and similar safeguards to prevent unauthorized access through the Internet.

The measures to detect attempts to commit computer crime include:

1. Logging and follow-up of exceptions. The system should be designed to log unusual activities, and procedures should be in place to follow up on reported exceptions, such as—
   - Transactions that are out of sequence, out of priority or otherwise out-of-standard.
   - Aborted runs and entries, including repeated attempts to unsuccessfully enter the system.
   - Attempts to access applications or functions beyond a person's authorization.
2. Logging and following up on variances that indicate a problem may have occurred or is occurring.
3. Awareness of employee attitudes and satisfaction levels.
4. Sensitivity to reports that particular individuals are having problems, living beyond their means, or talking about *getting even* for perceived slights.
5. Use of newly developed *intrusion detection systems* that use artificial intelligence capabilities to detect unusual transactions flowing through a system. These are evolving and have the prospect of being an order-of-magnitude improvement in crime detection technology.

8.6.4 Security Countermeasures to Computer Crime

The focus of chapter 4 of this Handbook is computer security in general. The focus of this section is the specific measures that are often used to prevent computer crimes by those either inside or outside an organization. While some measures are applicable to almost all situations, it is vital that each organization consider those controls that are appropriate to its particular circumstances.

Security Holes

One of the unpleasant realities in today's systems environment is that the systems we use, including operating systems, firewalls and security packages, and application systems, are not perfect when they are released by the manufacturers to their customers. On a continual basis, security problems are discovered. Information about ways to exploit security *holes* is quickly reported worldwide by independent bulletin board systems, government-funded sites (such as the U.S. Computer Emergency Response Team at Carnegie-Mellon University), and the manufacturers. Sometimes the problem and the ways to exploit it are reported before a repair patch can be developed. It has become, therefore, absolutely vital that every organization monitor these information sources to be certain that all relevant holes in security are understood and closed as soon as possible.

If the hole is not closed, and experience indicates that this is often the case, a company can continue to operate with known holes in its security. It is also vital that the internal auditors understand the importance of monitoring and closing software holes, and that this is included in the review plan.

Computer Access Control

Controls that allow only authorized people access to sensitive systems include—

- *Passwords.* Use passwords that are long enough to be difficult to guess. Passwords should not comprise simple words, names of relatives, and so on, and should be changed regularly.
- *Compartmentalization.* Restrict users to the specific files and programs that they have a job-related need to access.
- *Use of biometrics.* Use fingerprints, iris recognition, hand geometry and other new technologies for added measures of control.
- *Use of one-time passwords.* Use hardware or software that generates a new password for each access.
- *Automatic log off.* Use this measure to prevent unauthorized access to the system when authorized users fail to log off.
- *Time-day controls.* Restrict personnel access to those times when they are supposed to be on duty. An extension of this concept for companies using automated time-clock systems is to deny access and report a violation if access is attempted when an employee is not shown in the time clock system as being present.
- *Dial back systems.* Use these systems when access is through a dial-up system. On accepting a user ID and password, the system hangs up and dials a preestablished number at which the approved user is standing by. This is very helpful when a person works at a predictable location, for example, the home office of a telecommuting employee.
- *Random personal information checks.* Implement this means of identifying unauthorized log-in attempts. The system randomly transmits a question that only the authorized individual could answer and denies access unless the right answer is received. If several dozen personal questions are on file, this technique can be very useful.
- *Internet authentication.* Use this control for telecommuting employees. With telecommuting on the rise, many companies are taking advantage of low-cost, high-bandwidth Internet connections, such as Asymmetric Digital Subscriber Lines, which offer download speeds of up to 1.5MB per second and uploads of 400KB per second for nominal monthly charges, which includes continuous access, twenty-four hours a day, seven days a week. This technology, which identifies a specific Internet user and sends information across the Internet securely, is rapidly evolving.

8.6.5 Solutions

When investigating computer crimes, investigators and forensic accountants often discover what could have been done to prevent the crimes. The following are some of the most frequently found items. The organizations failed to:

- Have written policies and security rules for the use of computers and systems.
- Have temporary employees and independent contractors follow the same security rules as regular employees.
- Adjust access as people changed responsibilities internally.

- Keep up with and close security holes in applications, firewalls, and operating systems.
- Maintain virus protection on a fully updated basis.

Some of the suggestions to improve computer security include implementing:

- More effective policies for security over proprietary information.
- Better interaction between the human relations, systems and security functions.
- Better internal accounting controls.
- Better supervision of those with sensitive access to systems.
- Better education of computer users regarding security.
- Better computer audit software.
- Better software security.
- Better physical security in the workplace.

8.7 Selected Computer Crimes

8.7.1 Brief Case Synopses

It is useful to look at actual cases of computer crime to see the challenges businesses face if targeted by an offender. In each of these brief case studies, consider how your organization's existing security system would have faired, how your own organization would have reacted, and how likely it is that your current system of internal controls would have identified the problem and traced it back to the guilty parties.

ER Fraud Case Study

A computer operator at a hospital was charged with embezzling $40,000 by submitting false invoices that were processed through the hospital's computer system. At the same time, the hospital's assistant data processing manager accepted a $41,000 bribe from a consultant who stole an additional $150,000 by submitting false invoices for computer services. Both the operator and the assistant manager had prior convictions for computer-related crimes. Because computer personnel were not directly involved in patient care, hospital policy did not require a background check. An inexpensive reference check with previous employers could have possibly prevented the crime because the offenders would probably not have been hired when it was revealed that they had falsified their employment applications.

Even Experts Have Bad Days Case Study

A partner at a major international consulting firm received an anonymous call suggesting that one of the firm's senior information systems managers was defrauding the firm through a scheme involving false invoicing for supplies like laser toner cartridges and backup tape cartridges. A confidential internal investigation was carried out and no problems were revealed. Every invoice could be shown to tie directly to the actual material that had been delivered. The report seemed to be false, but a member of the firm's management committee decided that someone independent of the company should take a second look. Investigators were hired and they discovered that the material had been delivered, but they could find no record of the firm that supplied the materials. A simple background check on the vendor showed that it was just a shell formed by the senior information systems manager. He had developed a scheme in which he would place orders with the shell company (actually, with himself) and then order the same material from a reputable supplier who sent it to his home overnight. He would open the boxes, remove the original vendor's invoices, insert his own invoices (which were exactly 15 percent higher than what he had paid) and then he reshipped them. This simple scam resulted in a loss to the company of more than $300,000.

As shown in this case, vendor fraud can occur even in situations when all of the materials were actually received. No employees had questioned why so many orders were being placed with a company no one had ever heard of when major vendors could provide the same material in less time and at a lower cost.

The Invoice Looked Good Case Study

The scam was brilliant. The accounting manager had found a way to get his employing company to pay for his gambling losses in Las Vegas. Every time he needed to send a payment, he simply created an invoice for services at some distant office. The invoices were always from different companies, but on all of them he put a stamp on which he wrote their vendor number in the company's system. Of course, the vendor number was one the accounting manager had assigned to the holding company that owned the casino. Of course the casino was always glad to see him on his quarterly visits: it didn't care whether the check was made out to it or to its parent company. Because the computer system wouldn't reject the invoice as long as the vendor number was valid, the computer generated the check in the weekly check run; it was signed by another machine, and mailed out with thousands of other checks.

The scheme worked for years, until the outside auditors decided to conduct an internal control review, and determined that there was no match between vendor names on invoices and vendor numbers. In checking a vendor list, one of the auditors recognized the name of the casino's parent company, and wondered why this unlikely organization would be a vendor. The manager told the auditor that the company held meetings at the casinos owned by the company. Unfortunately for the manager, the auditors checked his story, and the scheme was revealed.

Breaking the Bank Case Study

A European bank sustained losses estimated at $65 million over a two year period when the head of the foreign currency transfer department and her assistant, who had broken the bank's computer transfer codes, were able to move money into outside accounts. The fraud was discovered through an audit, and the two perpetrators were arrested. Afterwards, everyone questioned how it was possible for such a large amount of money to be stolen with no one noticing and raising the alarm. Further investigation showed that the bank was involved in complex money laundering and tax evasion activities. Apparently the two managers believed that with all of the manipulation going on, no one would notice their independent scheme, and they were almost correct.

A New Form of Fraud Case Study

An employee of an insurance company in Florida had the dubious honor of being one of the first people convicted under that state's computer crime law. The employee was a benefits clerk with the company, and used her expertise in the company's systems and procedures to steal more than $200,000 in two years. She filled in the forms that benefits examiners used to approve claims and entered them into her computer terminal. She used a variety of names and policy numbers–all real–and created the paperwork to back up the claims. Her mistake was always using, as the mailing addresses for the checks, one of three addresses: her own, her father's, or her boyfriend's. The security department of the company discovered the fraud by looking for unusual patterns of payment addresses.

Welfare? It Was for our Own Welfare! Case Study

It may be impossible to discover exactly how much they stole, but a State Department of Social Services learned that one of their supervisors worked in collusion with a clerk to steal $300,000. This was a simple matter of input falsification. The clerk and supervisor submitted dozens of false claims for benefits and collected the payments. The fraud was discovered when a data input clerk noticed that the authorization data on one of the forms she was entering was incomplete. She called the eligibility worker, whose signature had been forged by the supervisor, to check on the incomplete form. When that person denied authorizing the claim or signing the form, an investigation was performed and the fraud was discovered.

When Time Stood Still Case Study

Wouldn't it be great to get the results of horse races before they ran? Imagine always betting on long shots when you know the winner. Just a dream? Not for the computer operator at a government-run betting agency in Australia. He figured a way to reverse time. Just before certain races, he reset the system clock to read three minutes earlier than it actually was. As soon as the race was run, he called his girlfriend, who was an off-track telephone betting clerk. She immediately entered bets on the winner. Because the computer believed that the race had not yet started, the bets were accepted. Then, the operator would reset the clock. Unfortunately, we can't report that the scheme was uncovered by brilliant work by internal auditors, external auditors, corporate security personnel, or even brilliant police work. The operator's girlfriend turned him in when she discovered he was seeing another woman.

8.7.2 Case Study: A Closer Look

There are thousands of cases of serious computer crimes on the books. Some were presented in the previous section. To provide a closer look at the way these cases are investigated, one full-length case study is included. This case involves deliberate actions by an insider who disrupted the email capabilities of an organization.

The Case of the Suicidal Computers Case Study

It happened, as do so many unpleasant things, in the dark of night. A dozen computers—each dedicated as an email router for a major financial services firm—apparently made a mutual decision, precisely at 5:00 A.M. one morning, to commit suicide. At that time, each of the computers suddenly and without warning, proceeded to completely reformat each of their hard disk drives. From that moment on, email within the huge global organization stopped. Any message that went outside of the local office was not going to be delivered.

Within an hour, the problem was noticed. Within two, it was apparent that the problem was not small and was not going to be easy to fix. Because many of the important daily operating communications of the company went through email, it was clear that a back-up plan would be needed to replace the damaged communications links. While one group of managers developed a plan to keep the organization functioning, the Chief Information Officer passed the word to the company's communications manager to *fix the problem.* The data communications manager immediately contacted the manufacturer. Because the organization was a large and valued customer, the manufacturer put two systems engineers on the next available flight.

At the same time, the Director of Corporate Security recognized that, while it was possibly an accident—perhaps a programming bug—that caused this crisis, it was probably a deliberate act of sabotage. If it were, he knew he would need proof to determine who had caused it. The Director of Corporate Security also understood that proof requires evidence that could be admitted in a court of law. Unfortunately, the director had previous experience in computer fraud cases in which *evidence* that might have existed was destroyed in the attempt to fix software problems. Therefore, two calls were made: The first was to the CEO of the company, who gave him authority to investigate the incident and, if it were shown to be deliberate, to identify and punish the perpetrator. The second call was to a private investigations firm that specialized in high-technology incidents.

The investigators understood that they could not interfere with the repair efforts; nevertheless, they immediately went to the data center. They briefed the repair team, and made a simple request: Please don't destroy or change anything that might be the cause of the incident without checking with us first, and keep detailed notes of your findings.

Over the two days it took to identify the problem and complete repairs, the investigators collected evidence, both in the form of software, and in written statements from the software engineers.

During the investigation, it was discovered that one email server had not reformatted itself. Because of a hardware problem, it had been shut down when the incident occurred. When the engineers discovered this, they examined the unit. One of the company's technicians noticed that the program that controls the processing of daily backups indicated it had been modified a few weeks earlier.

The technician who was responsible for backup knew that she had not changed the program in months. Yet the program had been changed. It still performed its normal backup, but there was a new routine that checked the date every time the program ran. On a specific date, the program had just two lines of code to be executed, and those two lines instructed the computer to immediately reformat its hard drives without warning, and without any report being generated. The investigators took possession of the server, since it was now apparent that the act was deliberate.

Over a forty-eight-hour period, the problem was solved, and all systems were checked for the existence of the deadly software. Before the engineers from the computer manufacturer left, the investigators assigned them one additional task. Using the notes they made during the previous forty-eight hours, each of the engineers wrote a memo documenting his or her findings in the context of what was now a potential criminal investigation. These statements were quickly reviewed, and then signed and sworn to before a notary. This action converted a memo into a sworn affidavit, which could have great value in any future court action.

With the email system back in operation, the data center management worked with the investigative team to determine who could have inserted the killer code into the dozen servers. Because of security measures built into the system, very few people had the authority to make those changes. In fact, the investigators were told, only four employees had that authority, and all were exemplary employees, so far beyond suspicion that no one could conceive of any of them having done this. Yet it had to be one of them. Who else could it be?

That was the question put to the head of the email management group, where the four suspects worked. She was convinced that none of the four employees were responsible; however, she had another candidate under consideration. He had resigned some weeks earlier, but, as a member of the group, he would have had the authority. Why had he left? Because he felt that he was misunderstood and insufficiently appreciated. He believed he knew far more than the others in the group, including the group head, about email technology. He had publicly gone to senior data center management to request a promotion to group head. When his managers decided that they would keep the present manager, this disgruntled employee had given notice, telling others that the company did not deserve him.

An examination of the former employee's computer revealed evidence of the destructive code that had caused the shutdown. There were several versions of the code found, including the key line that delayed the destruction until several weeks after he left the company. On the evidence presented by the investigators, the case was referred to law enforcement. The police accepted the case and reviewed the evidence. The case was brought to the county prosecutor, who determined the actions to modify the computer's program were a violation of the state's computer crime laws and that he would prosecute.

8.8 Conclusion

One of the peculiar things about the field of computer crime is that one can say almost anything and go unchallenged. The only thing people seem to agree on is that most computer crime is probably never reported, either because it is never discovered or because the company is embarrassed and chooses to handle it administratively. Often the company will forego prosecution if the offender resigns and agrees to never discuss the incident. This is why people who commit computer crimes can, in effect, get away with it and go on to another company with their reputations apparently intact.

In this chapter, we've tried to show that it does not require tremendous computer skills to commit a computer crime. Any employee, temp, or independent contractor with authorized access, as well as anyone with unauthorized access, can do it. Since most computer crimes involve input or output manipulations, the individuals most able to commit these crimes are not developers but employees in departments that use the systems. This is not to say that systems people don't commit computer crimes; they do but they are not typically likely to do so.

We have also tried to show that the commonly held belief that most computer crime is committed by outside hackers, who gain access to systems through almost mysterious abilities, is also a myth. Most of the incidents involve actions by insiders. Again, some occurrences do involve those outside of the organization, and defensive systems, such as firewalls, are absolutely necessary.

A third myth is that computer-related thefts, including fraud and embezzlement, are not detected by audit, but by accident. If that were true, and it is not, it would imply that the criminals are somehow more intelligent or more skillful, or perhaps more cunning than the noncriminals, and this is not the case. Good internal security, accounting and audit systems are very effective and do catch the bad guys. It is when these controls are *not* in place or when they are not implemented with sufficient resources, that the criminals get the upper hand.

As computer security becomes an increasingly important aspect of technology, it is likely that better mechanisms to prevent and detect computer crimes will evolve. But to gain the needed protection, it will be necessary for companies to adopt the technology and to implement it properly. Again, those who fail to assign sufficient resources to prevent the problem are destined for problems.

Finally, remember that once a security weakness is identified in a system, whether by hackers or security experts and the knowledge of the hole becomes public, it is important that it be closed quickly. There is nothing more discouraging than having to tell a victim that it was hit by a perpetrator who used a well-known hole to enter its system, and that all along there had been an easy-to-install, free patch out there, but that it was never installed.

Dealing With a Known or Suspected Fraud

CHAPTER 9:

Dealing With a Known or Suspected Fraud

CHAPTER 9:

Dealing With a Known or Suspected Fraud

9.1 OVERVIEW

9.1.1 Purpose and Scope

The primary focus of this Handbook is fraud prevention, not fraud investigation. Likewise, this Handbook is intended primarily for the CPA, whether in public practice or in industry, who is responsible for fraud prevention, rather than the full-time fraud investigator. However, professional fraud investigators will also find this Handbook useful in many ways, and occasionally there may be some crossover between the two functions; nevertheless, the distinction between the two is an important one. Prevention cannot come without an understanding of how fraud is perpetrated and the means by which it is concealed. To reach this understanding, it is necessary to have a firm foundation in fraud investigation techniques.

The experienced fraud investigators achieve their status through professional training and, most important, extensive experience in the investigation of fraud. It is well beyond the scope of this Handbook—indeed, it would be a virtually unachievable goal for any text—to synthesize the knowledge and expertise gained by an experienced forensic and investigative CPA over many years. There is simply no substitute for experience.

Nevertheless, virtually all CPAs should be concerned with fraud prevention, investigation and reporting, whether internally to an employing company, to a client, or to a court. Occasionally and despite the best fraud prevention efforts, a known or suspected fraud situation may surface. It is important in such circumstances that the CPA—

1. Be capable of acting competently: that is, perform the acts that should be performed and avoid or not perform those acts that should not be performed.
2. Understand the role of the forensic accountant and others who may be called in as part of the fraud investigation.

This chapter should serve to introduce the CPA to fraud investigation and reporting. It is not intended as a substitute for professional expertise in fraud investigation. Until the requisite experience is gained, in all cases involving fraud or suspected fraud, the inexperienced CPA should seek the assistance of a lawyer knowledgeable about fraud and a CPA experienced in forensic accounting.

9.1.2 Forensics and Forensic Accounting

The term *forensic* can be defined as, "belonging to, used in, or suitable to courts of law." This term describes the standards that are applicable to the discipline in question—that is, a forensic medical examiner would conduct autopsies to a standard required for court purposes, and a forensic accountant would conduct financial analyses to a standard required for court purposes. Thus, a forensic accountant may also be involved in civil litigation cases, which do not necessarily involve fraud.

But what is that standard? Generally, the forensic standard involves considering all the relevant evidence that could affect the professional's opinion and yet withstand rigorous cross-examination from counsel who is keen to undermine or disprove the professional's opinion so that the professional can properly assist the court reach its decision. It also involves a strong understanding of the legal system.

It follows then, that *forensic accounting* is a discipline involving accounting to a standard required by the court—the criminal and civil courts, as well as arbitration, mediation, and other forms of business dispute resolution that require expert evidence to a similar standard. It involves the application of financial skills and an investigative mentality to unresolved issues, conducted within the context of the rules of evidence. As a discipline, it encompasses financial acumen and a strong knowledge and understanding of business reality and the workings of the legal system. In the context of a fraud case, extensive fraud investigation expertise is essential. Its development has been primarily achieved through on-the-job training, as well as experience with investigating officers (in fraud cases), legal counsel and in the courts.

Accounting practitioners who concentrate their professional practice on matters requiring them to testify in court as to the findings from an investigation of accounting and financial evidence are termed *forensic accountants.* The ultimate test for the forensic accountant is acceptance by the courts of law—both criminal and civil—of him or her as an expert witness providing testimony in the area of accounting and financial matters.

While the American Institute of CPAs and the state Boards of Accountancy currently do not prescribe any standard specifically related to forensic accounting, it is clear that the standards for this practice are determined in the first instance by the courts of law. At the same time, a CPA is required to meet the general standards of professional practice as stipulated by the governing State Board of Accountancy and American Institute of CPAs.

9.2 The Five-Step Investigative Approach

Typically, there are five major steps in the forensic accounting and fraud investigation process:

1. Planning.
2. Gathering evidence.
3. Analyzing and testing.
4. Reporting and testifying.
5. Case Resolution.

For a more detailed checklist, see the table at the end of this chapter.

9.2.1 Planning

As with almost all endeavors, planning is critical. A well-planned investigation maximizes the chances of success; poor planning can lead to disaster. In the early stages of a forensic accounting or investigative engagement, it's especially important to (1) establish the scenario, (2) identify areas of concern and uncertainty, and (3) define the nature and scope of the investigation.

Establishing the Scenario

The amount of information available during the earliest phase of an engagement will vary from case to case. Establishing what is known is of special importance. This is true because it has a direct impact on the nature and scope of the investigation.

A known or suspected fraud almost always comes to light through one of the following three broad scenarios:

1. *Accounting irregularities.* One of the most common irregularities is a discrepancy between the book value of an asset and its value as determined through physical counts or confirmations. For example, a physical inventory count may reveal a major shortage compared to the perpetual inventory records, or accounts receivable confirmations may reveal much lower values than the accounts receivable subledger. Other common examples include bank reconciliations that do not balance, and complaints from customers that their statements are incorrect. Any irregularity that comes to light during an internal or external examination would also fall into this category. The common theme in all of these examples is that the company's records—its information system—have raised a red flag that signals the possibility of fraud.
2. *Immediate physical evidence.* Physical evidence may be readily apparent or uncovered upon inspection. Obvious examples include the aftermath of sabotage or arson. Human or electronic surveillance techniques might also yield immediate evidence (for example, with respect to employee theft or the diversion of inventory).
3. *After-the-fact incriminating information.* Incriminating information is a grab-bag category that comes in various incarnations: outright confessions brought on by guilt, anonymous tips, memos in brown envelopes, whistle-blowing employees, irate spouses looking to get back at their fraud-perpetrating husband or wife, honest citizens just trying to do the right thing, and so on.

In any fraud investigation the first step is to establish which of these three scenarios exists, and the nature and scope of the related evidence.

Identifying Areas of Concern and Uncertainty

The next step in the planning phase is a blending of the Boy Scout motto: *be prepared* and Murphy's Law: *whatever can go wrong, will.* Immediate areas of concern depend on the scenario identified in the previous step. Dealing with sabotage requires the immediate beefing up of security at other likely targets to prevent further damage. Dealing with a specific employee who is suspected of fraud—such as an accounts receivable clerk who might be perpetrating a lapping scheme, or a shipping department employee misappropriating inventory—you would want to secure all possible evidence and remove the suspect employee from the scene. Removing the employee from the scene need not be done in a direct, accusatory way. For example, if the fraud red flag is not common knowledge among the work force, the employee could be sent on a week's training course.

Beyond the immediate concerns of asset protection and evidence preservation, it's important, to the extent possible, to identify the uncertainties in the investigation—any pieces of the puzzle that are missing, so to speak. What are the major strengths and weaknesses of the existing evidence and supporting material? What additional evidence is likely to be available? What additional research, investigation and analysis are likely to be required to obtain any needed additional evidence and make it useful? Without at least a rough idea of where you're going, you most likely will not arrive at any valid conclusions.

Perhaps most important, you should think of any constraints, obstacles and pitfalls you are likely to encounter along the way. Obviously, forensic accountants and investigators need to be concerned about legal constraints in conducting their investigation. For example, as a general rule, only law enforcement authorities in possession of a valid search warrant can legally search a residence or a vehicle. (There are several exceptions, but for practical purposes none of them would apply to a fraud investigation.)

Less clear may be situations such as searching employee lockers. Judicial authorities have established that if employees have been put on notice all along that their lockers are subject to inspection, they probably can be searched. If this notice is lacking, legal counsel should be consulted, which should be the rule followed in all cases. Other concerns of investigators include lawsuits for false accusations or wrongful dismissal, and constraints imposed by collective bargaining agreements. The point is that a fraud investigation can be a legal minefield that must be navigated very carefully and deliberately, not haphazardly. To keep from hitting a mine, the safest course to set is early consultation with appropriate legal counsel and an experienced forensic CPA.

In addition to legal constraints, factors such as the company's reputation and relationship with its employees must be considered. For example, you would not want to alienate all your employees through hasty implementation of draconian investigative or security measures, just because of one bad apple.

Defining the Nature and Scope of the Investigation

The last step in the planning phase is to define the nature and scope of the investigation. This should be a fairly simple and straightforward process if the first two steps—establishing the scenario and identifying areas of concern and uncertainty—were properly thought out.

The nature and scope of the investigation are defined by several interrelated attributes including—

- The nature of the main objective—for example, prevention of further incidents, dismissal of the perpetrator, proving the case for criminal prosecution, establishing a loss claim, and so on—and the ranking of the objectives when there is more than one.
- If a criminal prosecution is envisaged, the point at which to involve the police.
- The level of secrecy or *cover* required in conducting the investigation.

For example, if the scenario involves an anonymous but seemingly credible tip implicating a purchasing employee in a kickback scheme, the objective may be to prove the case for criminal prosecution. The nature of the investigation will be fairly secret, because the parties involved are unlikely to confess and you would not want to alert them to the investigation. Because kickback (that is, secret commission) cases can be difficult to establish, the scope of the investigation could become extensive, including background investigations of both the bribe giver and bribe taker, surveillance, and possibly even setting up a sting operation.

9.2.2 Evidence Gathering

Once the planning phase is complete, the general objectives of the investigation must be translated into specifics, for example, identifying the documents and other information to analyze, conducting interviews, and obtaining third-party information required for corroboration.

Throughout the process, two important questions to keep in mind are what logical alternative interpretations exist for the evidence, and what eventual use will be made of the evidence. In particular, the forensic accountant must be able to understand the difference between relevant and irrelevant information, and must be willing to apply the standards of evidence required by the court.

Information Gathering Techniques

The forensic and investigative accountant is not a police officer. He or she does not have the resources of a police officer and, even when working to assist the police, must work within his or her own expertise, and within the rules governing professional conduct. Among the most important investigative tools are those that enable the forensic accountant to gather and analyze information available in the public domain in conjunction with other information gathered during the investigation.

For example, in investigating an individual, it may be possible to gather background information concerning certain aspects of an individual's financial circumstances (for example, mortgages and other secured debts, old court judgments, and so on), educational and employment references, professional qualifications, and other details such as whether he or she has taken his or her annual vacation. Also worth exploring is corporate information such as jurisdiction of incorporation, authorized share capital, and the identity of all officers and directors since incorporation can often be obtained from the appropriate state office, usually the Secretary of State of the jurisdiction where the incorporation took place. In some jurisdictions, shareholder identities can be obtained. In many instances, private offshore corporations have less information available than publicly traded North American companies.

Public domain information may also provide critical clues or evidence. For example, comparison of a company's statistics and trends to others in its industry, that is, benchmarking, may identify unexplained variances that alert the forensic accountant to possible questionable activities or that warrant further investigation. At the very least, the background data will provide context for the detailed findings from the examination of nonpublic data.

There are many sources of public information about organizations, industries, and institutions. Very often a university reference library or a government resource center can provide access to documents, reference textbooks, computerized databases, and other sources of information that can assist in understanding and analyzing a case.

Documentary Evidence

At the beginning of any case involving documentary evidence, there are two key questions. What documents should be obtained? And where will they come from? These questions are usually resolved after discussions with available witnesses and an initial assessment of the findings to date. Depending on the circumstances, it may be necessary to involve the authorities to obtain a search warrant or begin legal proceedings so that a court could order the seizing of documents.

The main goal is to gather all documents that might be useful, bearing in mind that irrelevant documents can always be returned to their proper place. It is necessary to decide, in consultation with legal counsel, whether to be selective (that is, review all documents but take only those deemed necessary), or whether to remove or secure all of the documents from the premises by taking the filing cabinets, and so on. It is difficult to lay down hard and fast rules, but clearly the primary purpose is to obtain all documents that might be relevant without resorting to a *fishing expedition.*

The minimum requirements for financial documentation, for the period under investigation, are likely to be the following:

- Books and records, management reports, and statistical analyses pertaining either to the management of the company or to an individual.
- Documentation pertaining to the movement of assets into and out of a company.
- Relevant correspondence.
- Personal documentation, such as bank-account records.

Documents, including seized documents, should be properly identified and catalogued. Documents must be handled carefully. They should not be written upon, altered, stapled or unstapled during the course of the investigation. The investigating accountants, in particular, should bear this in mind.

Documents should be examined in detail and categorized as follows:

1. Documents required for evidence.
2. Documents required for rebuttal of the defense arguments.
3. Documents required for other reasons.
4. Documents that can be returned.

Once the documents have been sorted into these groups, photocopies can be made to provide working copies for the investigating accountant to use when preparing schedules, and in general for the working paper files.

Documents will subsequently be selected, from among those photocopied, for use in the presentation of evidence in a court of law. They should be compiled and assembled into a document brief.

Admissibility of Accounting Evidence

It is important during the evidence gathering stage to consider the two forms of documentary accounting evidence that may be presented in a court of law:

1. *Primary*, that is, the original, individual accounting documents obtained from the parties concerned or other sources.
2. *Secondary*, that is, summaries and schedules based on the original documents, which are produced by an accountant after examining the primary evidence.

The issue of whether secondary accounting evidence should be admissible has been argued in the courts for many years. Two opinions that allowed secondary accounting evidence, are described below.

In the first case, the court ruled, and was upheld on appeal, that a summary of documentary evidence was admissible. The court said, however, that the summary was in itself not evidence of the underlying facts; rather, it was strictly an aid to understanding primary evidence that had already been established. The judge made the following observations about the use of secondary evidence:

1. No more reliance could be placed on the survey than was placed on the primary evidence it was intended to summarize.
2. The summary did not prove the veracity and content of the primary evidence.
3. Any summary of primary evidence must show every weakness previously determined as existing within the primary evidence.

In the second case, the court ruled that an exhibit prepared by an accountant, based on the documentation before the court, be introduced into evidence because it helped to simplify and trace the many transactions previously discussed in the court. The defense was concerned that the exhibit expressed the independent opinions of the accountant who prepared the material and, therefore, was not objective. However, the judge ruled that any opinions reflected in the exhibit were opinions that were readily ascertainable from the documents themselves—the primary evidence.

Interview Techniques

One of the more important tools for the forensic accountant is the interview process—this is a complex subject area on which several books have been written, and which takes years of experience for forensic accountants to master.

For the purposes of this Handbook, rather than attempt to explain the entire process, this section provides highlights of a few of the skills involved:

- The interview process should yield evidence that is as clear, unambiguous and concise as possible.
- Each interview, in order to be effective, should be carefully planned regarding the issues to be examined. All supporting documentation relating to the issues in question should be readily available to the interviewer in the event that the documentation is needed for reference purposes during the interview.
- The forensic accountant should consider the timing of the interview in relation to the extent of evidence gathered to date. Usually, it is best to gather as much documentary and other evidence as possible before either confronting the suspect or suspects directly or alerting those suspects by interviewing a parade of witnesses in a highly visible manner.

- The forensic accountant should consider all the physical aspects relating to the venue of the interview—including the size, temperature and lighting of the room; the size and positioning of the furniture within the room; and the seats to be occupied by those attending the interview.
- The forensic accountant should be skilled at asking both open-ended and closed questions, and should be able to distinguish when these kinds of questions would be most effective.
- The forensic accountant must be able to differentiate between an inarticulate explanation by a nervous individual and the evasive explanation offered by an individual who does not want to have his or her actions or motives identified and examined more closely.
- Discourse analysis, which involves the analysis of a person's written and spoken words, is an increasingly used technique in addressing suspected fraudsters. The theory of discourse analysis is that every word, pause, and gesture is important. There are no slips of the tongue. Thus, changing tense from present to past or person from first singular to first plural could be a significant cue. Therefore, when taking a statement, whether written or oral, it is important to have every last quirk–ums and pauses–recorded. Discourse analysis, however, is not the end all: it is one of the tools available to the investigator.
- The forensic accountant must be able to control and direct the interview process to draw out further evidence, often from hostile or adversarial interviewees. Effectively, the forensic accountant applies his or her own knowledge of the human element to assist in this process.
- The forensic accountant must be expert at taking good notes.

Private Investigators

It may also be necessary to engage private investigators to conduct surveillance of suspected perpetrators, for example, to observe their activity and record their presence at various locations and times, including meetings with certain individuals.

Forensic accountants who regularly work with private investigators as part of their team should be consulted for a recommendation regarding how to use investigators effectively, and whom to use.

Search and Seizure Mechanisms

In criminal matters, law enforcement agencies often obtain a search warrant to obtain documentary evidence. The forensic accountant may assist them in specifying on the search warrant those accounting, banking and other records that are to be seized as evidence of fraudulent activity. Depending on the jurisdiction, the forensic accountant may also be named on the warrant to attend its execution at the premises to be searched, in order to help identify those documents that are to be seized as evidence.

In civil matters, depending on the jurisdiction, different search and seizure mechanisms may also be available. The forensic accountant could provide assistance in obtaining evidence through the use of a seizure order, granted pursuant to a court application. Under the court's supervision, an order would permit counsel to recover documentary evidence from the other party. This evidence could otherwise have been destroyed or concealed.

Similarly if there is a concern that the assets of an individual under investigation may be dissipated, an injunction may be obtained from a court. This injunction would prohibit the individual under investigation from conducting his or her affairs in a manner that would financially prejudice the other party in a case prior to the court rendering its decision.

The rules governing civil suits in most jurisdictions allow discovery proceedings, which include answering either orally or in writing questions under oath and the production of documents, or some equivalent process. During discovery, the forensic accountant can

(Text continued on page 11)

assist counsel in requesting documents to be produced by the other party and in determining questions to be put to the witnesses for the other party.

The Role of Computers

Over the years, the role of computers in investigations has increased exponentially; for example, the use of the Internet as a research tool and the development of faster, more efficient software to assist in the investigative process.

Investigative software now includes many packages that are designed to assist the forensic accountant, investigator or lawyer with his or her work. For instance, scanners can be used to scan in huge volumes of paper evidence that can then be searched via keywords or phrases and organized using a database for quick reference later in the case. Queries can be generated in a matter of minutes, which search through databases of millions of transactions, to identify the proverbial needles in the haystack. Similarly, specialized software is now readily available for procurement fraud investigation and to recover file fragments from personal computers.

The work product of the forensic accountant is also generated by computers and generally includes a written report accompanied by various supporting information—for example, document briefs, chronologies of events, accounting schedules (either summaries or analytical schedules), graphs and charts.

9.2.3 Analyzing and Testing

During the analysis stage, the financial issues being investigated are evaluated in detail. Appropriate conclusions are drawn, either in terms of a finding of fact (for example, whether a particular transaction or event took place) or the resulting quantification of the alleged fraud. If the investigation has been properly planned and appropriate evidence is available and has been gathered, this step should go fairly smoothly.

The ultimate test of the evidence may come when the perpetrator is confronted with it. A trained interviewer in possession of all the facts can often elicit an immediate confession from an unprepared suspect. In many cases, the suspect is relieved that the matter is finally over because he or she no longer has to endure the stress of covering up the fraud.

Of course, there are many cases that are not resolved as quickly, proceeding instead to lengthy civil or criminal court challenges. The planning, evidence gathering, and analyzing and testing phases of the investigation must yield a product that, in the end, can withstand the court challenges.

9.2.4 Reporting and Testifying

The forensic accountant must be able to present his or her findings in a way that is understandable, and must do so in an appropriate format. The *American Institute of CPA Practice Aids* should be referred to when preparing the final report. In general, however, the appropriate format might be one of the following:

- A reporting letter, for example, a communication to counsel outlining the scope of the review and findings.
- An affidavit or deposition, that is, a sworn statement of findings with supporting documentation.

- A formal communication to the court, such as a report that sets out the forensic accountant's opinions and underlying findings, and that provides details as to how those findings are substantiated.

Often the findings must be communicated through oral testimony in court. Once again, that is why every phase of the investigation up to this point must be conducted with the legal evidence standards in mind. Forensic accountants must be prepared for examination under oath about all their activities. This examination can come at any time and in any form, for example, as an affidavit, a deposition, or oral testimony at the actual trial. They must be able to qualify as an expert witness based on their education, experience and knowledge. Finally, they must be prepared to respond to cross-examination and to the submission of different financial evidence and alternatives by the other side.

Keep in mind that conventional accounting evidence is only one part of a much larger pool of evidentiary material, which includes one or more of the following:

- Testimony of witnesses.
- Police witness interview notes.
- Statements of claim.
- Statements of defense and counterclaim.
- Examinations or production of documents relating to a civil matter or search warrants.

Additionally, the forensic accountant may carry out research to identify any precedents that may assist in reporting and presenting evidence.

Preparing and Presenting Accounting Evidence

Certain guidelines should be considered when preparing and presenting accounting evidence. Although set out primarily from the point of view of the investigator or legal counsel, forensic accountants (especially those who act as expert witnesses) should also be aware of these guidelines, which include:

1. Make yourself fully aware of the evidence, or lack of it, from an accounting standpoint:
   a. Be aware of the strengths and weaknesses of the case based on the available documents.
   b. Be aware of any investigation that may be needed to complete the accounting picture.
2. Thoroughly familiarize yourself with the final *accounting picture* as set out in the accountant's report, schedules, and document brief.
3. Decide what accounting evidence to call, if any.
4. Prepare evidence for the court:
   a. Request that the accountant prepare the appropriate report, schedules, and document brief.
   b. Request that the accountant prepare appropriate visual or other aids.
   c. Make available, as required by the rules of procedure, to the other side accounting material including the report, schedules, and document brief.

d. Accomplish the following at the meeting with the other side.
   - Explain the accounting material.
   - Ensure that there is an opportunity for explanation and production of documents by the other side.
   - Consider the admissibility of accounting material without formal proof.

5. Conduct a final pretrial witness interview of the accountant:
   a. Ensure that all documentation is introduced as exhibits.
   b. Confirm that the accounting schedules are properly cross-referenced to the document brief.
   c. Review the format of the examination of expert witnesses, including:
      - Areas to be covered.
      - Sequence of examination.
      - Exact nature of opinion evidence, if any.
      - Use of visual aids.

6. Make final preparations for tendering the accountant's evidence in court:
   a. Place exhibits in proper numerical order.
   b. Index the accountant's document brief with exhibit numbers.
   c. Confirm the logistics of using visual aids.
   d. Confirm the availability and legibility of copies of accounting schedules and visual aids.

Qualifying as an Expert Witness

The simulated testimony reproduced below shows how a CPA's qualifications as an expert witness can be established.

Examination—of Mr. I.M. Sleuth, CPA by Jim Jones, Esq. (Prosecutor)

Q. Mr. Sleuth, where do you reside, sir?

A. I live in Bigtown, Megaplace.

Q. And what is your occupation?

A. I am a CPA and a Certified Fraud Examiner.

Q. And do you practice on your own or with someone else?

A. I practice in partnership with other CPAs under the firm name of Sleuth & Company.

Q. And how long have you been operating the accounting partnership?

A. Close to twenty-two years now.

Q. And prior to that were you associated with any other firm?

A. Yes, prior to that I worked for a period of six years with a national firm following my graduation from school.

Q. And in what year did you qualify as a CPA?

A. In 1972.

Q. And since that date have you had occasion to testify in court with respect to accounting matters?

A. I have.

Q. And approximately how many occasions would that have occurred on?

A. An estimate of some fifty occasions.

Mr. Jones: Your Honor, I offer Mr. Sleuth as an expert witness on the basis of his qualifications that I have elicited.

Mr. Green (Defense Counsel): No objection, Your Honor.

His Honor: Thank you.

Q. Mr. Sleuth, I understand that you have prepared a number of documents relating to various transactions dealing with Acme Manufacturing?

A. Yes, I have.

Q. Mr. Sleuth, I show you a document, a rather large document, marked Exhibit A. I would ask you to look at that document and tell me if you recognize it?

A. Yes, I do.

Q. And did you prepare that document yourself?

A. Yes, I did, with the assistance of staff under my direct supervision.

Q. And I wonder if you would hold it in such a way that the jury will be able to see the structure of that document itself. It appears to consist of a number of columns, vertical columns, am I correct?

A. That's correct.

Q. And the document is headed what?

A. It's headed, *Analysis of Sales for the Period August 1, 1998 to October 5, 1998.*

Observing the Accountant Witness: A Positive Approach

The following list presents the ideal a CPA should, under the direction of legal counsel, strive for when giving oral testimony.

- The answers given should be responsive to the questions and as brief as possible, without losing sense.
- The statement of qualifications as an expert witness should be well outlined, factual, and not overly laudatory.
- There should be no show of bias when describing the scope and purpose of the services.
- The accountant should indicate the source of all documentation and acknowledge that all documents used to support his or her findings are currently before the court.
- The accountant should be prepared to consider new evidence provided it is relevant to the case.
- The accountant should be specific about the time period covered and the dollar amount of his or her findings.
- The accountant should be able to articulate the basis for his or her opinion in an organized and logical fashion that is easy for the judge (and if it is a jury case, a lay jury), to follow.
- The accountant should make good use of visual aids.
- The accountant should speak slowly and deliberately, leaving sufficient time for the judge (and jury) to absorb his or her evidence.
- The accountant should periodically check that the judge (and jury) is following his or her evidence.
- The accountant should direct his or her answers to the judge (and jury) rather than to the lawyer conducting the examination or cross-examination.
- The accountant should make a clear presentation.
- The accountant should be certain that the terms of the engagement are well organized and clearly set forth.
- The accountant should see to it that the accounting schedules are well referenced, including the visual aids, and can easily be tied to the supporting documents.
- The accountant should be calm and collected.
- The accountant should demonstrate knowledge of the documents and the case, and an understanding of the testimony of the other witnesses preceding him or her; that is, there should be a positive demonstration and total commitment and understanding of the matter before the court.

The Accountant Witness—A Negative Approach: What Not to Do

The following list presents the negatives an accountant can exhibit when giving testimony:

- Confusion.
- Lack of preparation.
- Self-described expert (that is, self importance: impressed with himself or herself and his or her credentials).
- The accountant demonstrates bias in the presentation and explanation of the scope and purpose of his or her services.
- Failure to present findings or conclusions.
- Lack ready notes in his or her file.
- Findings convey no definite time period.
- Findings convey no definite dollar amount.
- Poor visual image.
- Poor posture.
- Incomplete supporting documents.
- Argumentative and belligerent.
- Openly nervous.
- Off-hand answers to questions.

9.2.5 Case Resolution

Fraud is a crisis for an organization and its employees. Good crisis management demands that the investigative process not end with the reporting of findings or the giving of testimony. Briefly, this means the victim organization should—

1. Seek or enforce restitution from the perpetrator (for example, seize any assets pursuant to a court order).
2. Learn and adjust from the experience—in particular, ensure that controls are implemented to prevent a recurrence.
3. Keep channels of communication open between the crisis survivors—that is, the organization and its employees—to ensure the crisis does not damage their relationship or impair the organization's ability to function effectively and efficiently.
4. Implement regular, diligent monitoring and follow-up on the above points.

9.3 Forensic Accountants

Forensic accountants must possess a range of skills in order to carry out their investigations in a professional manner. These skills include not only thorough accounting knowledge but also knowledge of business and an awareness of the legal process. With these skills, the forensic accountant can investigate, analyze, document, report on, and testify as to the financial aspects of an investigation into a fraud or other so-called white-collar crimes.

In many instances, the forensic accountant may be requested to quantify the amount of a fraud loss in a criminal matter or the financial damages in a civil matter. While a criminal matter must be proven beyond a reasonable doubt, a civil matter must be proven by a preponderance of the evidence. Both require a demonstration of similar techniques and skills from the forensic accountant.

9.3.1 Professional Skills and Attributes

The seven major categories of a forensic accountant's professional skills and attributes are:

1. Accounting and audit knowledge, including good business knowledge.
2. Fraud knowledge.
3. Law and rules of evidence knowledge.
4. Investigative mentality and critical skepticism.
5. Psychology and motivation awareness.
6. Communication skills.
7. Computers and information technology comprehension.

A closer inspection of each category follows.

Accounting and Audit Knowledge

Professional training in accounting and auditing provides not only accounting and audit knowledge but also a practical understanding of business operations, business finance, corporate structure, industry practices, and standards of conduct.

The majority of those who identify themselves as forensic accountants are CPAs. These individuals have sought and found careers for themselves in an area that allows them to use their skills as CPAs, together with other personal attributes that are necessary in investigating business fraud and commercial crimes.

Audit skills are an important foundation for a forensic accountant. Due to the sensitivity of the work involved, forensic accountants must be able to focus on the need for a 100 percent substantive examination of all documentation related to a particular matter.

The accountant with good audit skills must have the ability to prepare and use complete and accurate documentation; thus the accountant must know how to catalog the available information. He or she must also be able to determine the other existing information sources, which initially may not be available but which can, with research and diligence, be uncovered, obtained, and utilized. With his or her accounting and audit skills, the accountant can inquire about, locate and identify investigation-related documents—whether they are present initially or obtained during the course of the investigation.

For most CPAs, audit experience includes both audit and nonaudit engagements covering a wide cross-section of business enterprises and their operations, from small sole proprietorships to large multinational corporations, both public and private. This familiarity with business enterprise is an important element in the forensic accountant's investigation of business frauds and similar matters.

Fraud Knowledge

In addition to professional training in accounting and auditing, the most important aspect of the forensic accountant skills mix is exposure to and knowledge of many different kinds of fraudulent transactions. This will allow the forensic accountant to identify red flags and to piece together patterns and theories that may otherwise elude an accountant who has not had the same degree of exposure to fraud.

Forensic accountants do not merely compute, they analyze. The analytical process is not an easy one, as each case is unique and therefore calls upon the forensic accountant's experience, formal training, and other important attributes. Specifically, he or she must be able to identify accounting problem areas, prioritize these problem areas or issues as required, and refine or change the focus of the investigation as new information is obtained and assessed. Often, an original theory may be only the beginning of an investigation, or it may be refined to a specific issue warranting further review. In providing assistance to the courts, this ability to properly focus the investigation is important.

The importance of experience cannot be overemphasized. The forensic accountant must also be able to look beyond the form of the documentation, to understand its substance and foundations, and to assess whether it is consistent with other business realities. The forensic accountant must understand the nature of the documents that he or she is reviewing and question their business reality. More than anything, a forensic accountant is distinguished by having "been there before." Knowledge of many different kinds of fraud, based on first-hand investigative experience, means a more effective plan of investigation, knowing when, how, and who to interview as well as the format for communicating findings in reports to clients and if necessary to the court.

Law and Rules of Evidence Knowledge

It is important for the forensic accountant to be knowledgeable about both criminal and civil laws, since these laws have a direct impact on matters involving the forensic accountant. Specifically, a forensic accountant must be able to understand both criminal and other statutes that may have been contravened, in order to identify possible issues. There is also a need to understand the rules of evidence to ensure that all findings are admissible in court, if necessary. Specifically, investigative accountants must have an understanding of the rules of evidence—for both civil and criminal matters—which consist of:

- What evidence is.
- How it is obtained.
- How it is preserved.
- How it is presented before the courts.
- How the forensic accountant's own work can become part of the evidence brought before the courts or before some other tribunal responsible for determining what has occurred.

To provide accounting assistance in a matter involving fraud, the forensic accountant must possess a general understanding of the issues by which the courts can judge an act to be fraudulent. He or she must be knowledgeable as to the court's tests for fraud—for example, the presence of dishonest intent as seen in the perpetrator's actions, or more particularly, the *mens rea* or criminal intent of the perpetrator at the time the act occurred. He or she must review and analyze accounting, banking, financial and other business records, and identify both specific acts and patterns of conduct that are suggestive of dishonest intent to deprive a victim of an asset.

Investigative Mentality and Critical Skepticism

The forensic accountant must possess an investigative outlook, tenacity, and the ability to identify indicators of fraud. Collectively, these attributes could be termed as the investigative mentality. This mentality encourages the forensic accountant to seek substance over form—to identify and analyze data and to conduct interviews to determine what has actually occurred in a business transaction, rather than what simply appears to have happened.

The investigative mentality is sometimes manifested by the *smell* test—the ability to assess relevant transactions or events to determine their reasonableness and to the extent possible, their veracity. In other words, in light of all the known facts, does a particular action appear reasonable and logical? Is the action or pattern of behavior plausible in the circumstances, or is there an *odor* that begs for further investigation?

The investigative mentality can also be thought of as professional, critical skepticism. It is not a shotgun approach; rather, it is a specific and precise set of judgmental procedures suitable for the circumstances that allows the forensic accountant to identify and assess all relevant facts and develop hypotheses. These hypotheses can then be researched further and tested more extensively as the investigation proceeds. The forensic accountant never discounts any aspect of an investigation on face value: Only after examining all available evidence and weighing its totality will he or she determine an item to be irrelevant to the issues at hand.

Another analogy—that of the watchdog-bloodhound—further illustrates the forensic accountant's investigative mentality attribute. A CPA is more akin to a watchdog—he or she looks for material misstatements in financial statements caused by error or fraud, but will respond affirmatively if warning signs of fraud appear through audit procedures. The forensic accountant, however, is more of a bloodhound—actively seeking out the presence of evidence, all of which when viewed together may indicate the occurrence of a fraudulent act.

While the investigative mentality requires a disciplined approach and a methodology, it also requires creativity in being able to identify and seek out further sources of evidence and to analyze this new information. Attention to detail is critical as the success or failure of the case may depend on the identification of evidence that, on initial review, may appear insignificant or irrelevant. The issues of materiality or sampling relevant in an audit assignment do not restrict a forensic investigation. Those restrictions may cause fraudulent acts to be overlooked, and they are inadequate in establishing evidence.

Psychology and Motivation Awareness

Another attribute of the forensic accountant is an understanding of the human element. Documents do not commit fraud; computers do not commit fraud; rather, people commit fraud. In assessing information, documentation and accounting records, one of the seasonings that the forensic accountant can apply to the mix is his or her understanding of individuals, including what motivates an individual to commit fraud and the attributes of an individual who commits fraud. This understanding, together with the ability of the forensic accountant to examine information not just from an accounting viewpoint, but also within the context of the overall picture or business reality, is important.

In general, it can be said that individuals react to satisfy needs. The forensic accountant must recognize the presence of such needs during his or her investigation, whether it is the need of an employee for greater income to maintain an extravagant lifestyle or the need of a sales manager to maintain sales volumes in a declining market so as to ensure his or her continued employment. Such needs often provide the motivation for acts that an employee may label differently but which are, in essence, fraud.

In a situation where an individual has both the need and the opportunity, a fraudulent act may be the result.

Communication Skills

Forensic accountants, as expert witnesses to the court in findings of fact, must be able to clearly and effectively communicate information. This means that they must be able to communicate without bias in written form, including the use of accounting schedules, charts, and exhibits. They must also be able to communicate to others the nature and extent of the work undertaken and the findings that have evolved from that work so that it can be understood both in a court of law and in other forums.

When the forensic accountant testifies as an expert witness in court, he or she must be able to explain the procedures, analyses, and findings of the investigation in such a way that the basis for his or her expert testimony—both facts and, if necessary, opinion—is understood by the judge and, if there is one, the jury. The forensic accountant's knowledge of the available evidence and possible alternate explanations of the events must be as complete as possible, to ensure that the findings are not compromised on cross-examination.

Understanding Computers and Information Technology

Today's computers have replaced yesterday's ledgers, and in fraud investigation it is important to be as up-to-date as the alleged perpetrators of fraud. Thus, the skills of a forensic accountant should include the ability to understand the opportunities computers provide to potential perpetrators of fraud as well as the ability to use computers in analysis and documentation of an alleged fraud.

Because succinct presentation to the judge and jury is so critical, knowledge of computer graphics is also helpful. The forensic accountant's findings often include quantitative analyses that are conducive to presentation in the form of graphs and charts that depict and summarize the information. Typical graphs and charts include summaries of the source and use of funds, as well as flow charts showing the movement of assets at various times.

9.3.2 Ethics

Independence and Objectivity

Independence and objectivity are integral concepts in the ethical training of CPAs. While the need for these attributes is well established in the audit area, they are extremely important in investigative work. The forensic and investigative accountant is not an advocate; rather, he or she provides the skills and input of an independent expert. Even a bias with respect to a single, small matter—whether actual or perceived—may call into question in the eyes of the court other unbiased evidence presented by the forensic accountant. He or she must therefore report objectively at all times.

Respect for Access to Information and Privacy Laws

One factor that must not be overlooked in the role of investigator is that the information that is gathered must be collected in an ethical and legal manner. One cannot misrepresent one's self when gathering information, nor can the process of collecting information be abused.

Most important, the rights of an individual whose activities are being reviewed must not be abused.

9.3.3 Kinds of Services Offered

Proactive versus Reactive Services

Forensic accounting services can be proactive or reactive. Proactive services include training on fraud awareness and fraud prevention measures, presented elsewhere in this Handbook. Reactive services are investigative and analytical in nature and are rendered after the event. Much of the information in this chapter addresses reactive services.

Civil versus Criminal Services

Another way to identify the kinds of services that a forensic accountant renders is to consider the forum in which a dispute is finally resolved. For example:

- A criminal forum must establish guilt beyond a reasonable doubt.
- A civil case has a less onerous burden of proof than a criminal case. The trier of the facts must reach his or her conclusion based on the preponderance of the evidence.
- A nonjudicial tribunal, for instance, an alternative dispute resolution proceeding (arbitration) can differ from a court of law by being either stricter or more lenient.
- Finally, if the circumstances are such that no reference is made to an outside tribunal, but rather two parties are to resolve a matter on their own, then the level of proof required is only what the other side will accept.

Other Categorizations

Services of a forensic accountant can also be categorized in other ways, for example by the type of procedures performed. These procedures can include—

- Performing an initial review of documentation to determine whether further research or investigation is required or necessary.
- Providing an affidavit or deposition outlining the results of a review of documentation.
- Providing a report identifying the scope of the work performed and findings.
- Assisting counsel in obtaining a search warrant (that is, in a criminal case).
- Providing expert testimony in court.

The nature of the industry in which a forensic accountant is performing an investigation can be another method of classification. For example:

- Service industries could include transportation, banking, securities brokerage, retail, real estate, construction, professional services (such as services of CPAs and lawyers), mortgage brokerage, and telecommunications.
- Manufacturing industries could include construction, farming, food processing, all forms of manufacturing, mining, petroleum, and publishing.

The above classifications could then be further refined, and others added. For example, government and nonprofit sectors are other areas where forensic accountants are called upon to provide their services.

9.4 CHECKLIST: DEALING WITH A KNOWN OR SUSPECTED FRAUD

CPAs can use the following checklist when dealing with a known or suspected fraud in their organizations or in those of their clients. ***No*** answers may require investigation and follow-up, the results of which should be documented. Use the *Ref* column to cross-reference the checklist to the appropriate work papers.

The checklist is intended for general guidance and information only. If fraud is of vital concern to an organization or if serious fraud is suspected, seek the advice of legal counsel and a CPA experienced in fraud investigation.

TABLE 9.1 DEALING WITH A KNOWN OR SUSPECTED FRAUD CHECKLIST

Dealing With a Known or Suspected Fraud Checklist	**Yes**	**No**	**NA**	**Ref**
1. **Planning**				
a. Has the main scenario of the fraud been established, including the sources of information pointing to fraud (that is, accounting irregularities, physical evidence, or incriminating information)?	☐	☐	☐	___
b. Have immediate areas of concern been identified, such as the need to protect assets from further damage (for example, by boosting security) and to preserve key evidence for further investigation (e.g., by removing the key suspect from the scene, through a leave of absence or other appropriate means)?	☐	☐	☐	___
c. Have legal and other constraints been identified, (that is, the provisions of any collective bargaining agreement) and has legal counsel been consulted?	☐	☐	☐	___
d. Has a preliminary assessment been made to determine:				
• The quality of the information currently available	☐	☐	☐	___
• Additional information that is needed	☐	☐	☐	___
• How to obtain the information	☐	☐	☐	___
e. Have the nature and scope of the investigation been defined, including:				

TABLE 9.1 *(continued)*

Dealing With a Known or Suspected Fraud Checklist	**Yes**	**No**	**NA**	**Ref**
• The main objective(s)	☐	☐	☐	___
• Whether (and when) to pursue criminal charges	☐	☐	☐	___
• The level of secrecy required	☐	☐	☐	___
• Administrative matters (for example, engagement letters; or if external forensic accountants are used, budgets)	☐	☐	☐	___
2. Evidence Gathering				
a. Has a detailed list been prepared of the evidence that is to be obtained or seized?	☐	☐	☐	___
b. Have all sources of evidence been considered (for example, books and records, documents, correspondence, public domain information, background financial information and personnel history, etc.)?	☐	☐	☐	___
c. When evidence is obtained, is it assessed for:				
• Relevance	☐	☐	☐	___
• Alternative interpretations (for example, simple error)	☐	☐	☐	___
• Eventual use and admissibility (for example, as court evidence)	☐	☐	☐	___
d. Are proper evidence-handling procedures in effect, (for example, taking photocopies; not writing on, altering, stapling or unstapling originals)?	☐	☐	☐	___
e. Especially for larger investigations, has evidence been categorized in a way that will facilitate its future retrieval and use?	☐	☐	☐	___
f. Has the nature, timing and scope of any interviews (especially of suspects) been carefully considered?	☐	☐	☐	___
g. Are interviews conducted by or with trained and experienced interviewers, with appropriate safeguards to prevent bogus harassment or other charges (for example, safeguards could include leaving the door ajar during interviews and having assistants interrupt at predetermined times)?	☐	☐	☐	___
h. When appropriate, has the use of reputable private investigators been considered?	☐	☐	☐	___
i. For any evidence to be seized, does the search warrant or court order have the proper scope so that all of the required evidence falls within its reach?	☐	☐	☐	___

(continued)

TABLE 9.1 *(continued)*

Dealing With a Known or Suspected Fraud Checklist	**Yes**	**No**	**NA**	**Ref**
j. Especially for larger investigations, have computer databases and other appropriate tools been used to store and cross-reference evidentiary materials?	☐	☐	☐	___
k. Has security over all evidence been established, including, if appropriate, off-site storage of copies (electronic, paper, or both) for key evidence and documents?	☐	☐	☐	___
3. Analyzing and Testing				
a. Has all evidence been systematically analyzed?	☐	☐	☐	___
b. Were appropriate conclusions drawn?	☐	☐	☐	___
c. Has the evidence been thoroughly checked and tested and reviewed with legal counsel to ensure it is up to court standards?	☐	☐	☐	___
4. Reporting and Testifying				
a. Has a forensic accountant prepared a well-organized, unambiguous report, summarizing the findings of the investigation?	☐	☐	☐	___
b. Has the report undergone a quality-control review?	☐	☐	☐	___
c. Has adequate preparation been done for testifying in court, including a full run-through?	☐	☐	☐	___
d. Is the person giving the testimony experienced, and if necessary, has he or she previously qualified as an expert?	☐	☐	☐	___
e. For expert witnesses, have fairness and impartiality, and the appearance of such, been present throughout the process (for example availability to both sides)?	☐	☐	☐	___
5. Case Resolution				
a. Has a plan and process been put into effect to seek and enforce restitution from perpetrators?	☐	☐	☐	___
b. Have controls and procedures been put into place to prevent a recurrence?	☐	☐	☐	___
c. Have channels of communication been kept open and other appropriate steps taken to maintain good employee relations and mitigate any other adverse effects of the crisis?	☐	☐	☐	___
d. Has a program been established to monitor the results of the above on an ongoing basis?	☐	☐	☐	___

Financial Statement Fraud

CHAPTER 10:

Reducing the Risk of Financial Statement Fraud

CHAPTER 10:

Reducing the Risk of Financial Statement Fraud

10.1 THE PERVASIVE NATURE OF FINANCIAL STATEMENT FRAUD

10.1.1 Overview

Financial statement fraud involves the alteration of financial statement data, usually by a firm's management, to achieve a fraudulent result. These altered financial statements are the tools then used by a company's managers to obtain some reward.[1] The reward may consist of direct compensation such as receiving a bonus that otherwise would not be paid without using altered, incorrect financial data to embellish management's operating performance. On the other hand, the compensation may be less direct in that managers avoid being fired for failing to achieve promised results. Compensation may also be indirect; for example, management may use fraudulent financial statements to raise additional capital that, in turn, allows a firm to expand and presumably enhance the value of shares held by management.

10.1.2 What Constitutes Financial Statement Fraud?

What constitutes financial statement fraud has been the subject of much debate because the lines between fraud and discretion are not always clear. It is easy to define fraud as a conscious effort by management to produce financial statements with materially wrong account data. It is almost as easy to identify as fraud misleading accounting entries that management cannot justify under any applicable accounting standards. Fraudulent acts become less obvious, however, when cloaked in the mantle of accounting standards that are incorrectly applied. For example, the applicable accounting standard in the United States is generally accepted accounting principles (GAAP) and those principles may allow management some discretion as to when to recognize revenue or expenses.

Honorable people can debate the most appropriate use of a principle when looking at the gray or more broadly permissive areas of GAAP. Less-than-honorable people, however, might make use of these gray areas to produce financial statements that mislead. This practice is found most often in concert with other misleading applications of GAAP.

Fraudsters almost always fail to discuss this choice of GAAP principles in the notes to financial statements.[2] Without knowledge of the impact of GAAP gray-area judgments on the financial statements, unsuspecting readers may mistakenly assume that revenues and

---

[1] In this chapter, the term *company* refers to any legal or business entity that prepares financial statements, including partnerships, limited liability companies, and corporations.
[2] Failure to disclose would be a GAAP violation; therefore, although the accounting for a certain transaction may appear to be supported by GAAP, failure to disclose so as not to make the financial statements misleading takes the company out of GAAP compliance.

expenses were accrued in a manner consistent with prior financial statements when, in fact, they were not. The end result may be that continuing operations appear to be profitable while, in reality, there may be serious problems that the misuse of GAAP gray areas can cover up for a short period of time. Thus, when accounting decisions purportedly in conformity with GAAP produce financial statements intentionally[3] designed to mislead the reader, those decisions cross the line into fraud.

10.1.3 SEC Definition of Fraud

These concepts are codified in the U.S. securities laws and regulations, especially Securities and Exchange Commission (SEC) Rule 10b-5[4], which states the following.

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or the mails, or of any facility of any national securities exchange,
>
> (a) to employ any device, scheme, or artifice to defraud,
>
> (b) to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
>
> (c) to engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

Publicly traded companies must conform to GAAP and to the rules and regulations promulgated by the SEC under U.S. securities laws. The SEC drew heavily on accounting literature when it recently addressed the issue of accounting gray areas. SEC standards (discussed below) that have their origin in GAAP will provide substantial guidance to determine financial statement fraud not only for publicly traded companies but also for all firms issuing financial statements in conformity with GAAP.

10.1.4 Common Methods of Committing Financial Statement Fraud

Research carried out for the Committee of Sponsoring Organizations of the Treadway Commission (COSO),[5] found the most common kinds of fraud were the following:

1. Overstatement of earnings
2. Fictitious earnings
3. Understatement of expenses
4. Overstatement of assets
5. Understatement of allowances for receivables

---

[3] As with proving any type of fraud, one must show that there was *scienter,* meaning that the fraudster knew that his or her actions were designed to mislead.

[4] Promulgated under Section 10(b) of the Securities Exchange Act of 1934.

[5] Mark S. Beasley, Joseph V. Carcello, and Dana R. Hermanson. *Fraudulent Financial Reporting 1987–1997: An Analysis of U.S. Public Companies,* published by COSO, 1999.

6. Overstatement of the value of inventories by not writing down the value of obsolete goods
7. Overstatement of property values and creation of fictitious assets

The following sections discuss the various kinds of financial statement fraud and the corresponding motives for each kind, the early indicators of financial statement fraud (both quantitative and qualitative) and the means to detect some of the most difficult-to-find kinds of fraud. At the end of this chapter, there is a checklist that addresses internal control issues designed to provide help in reducing the risk of financial statement fraud.

10.2 Kinds of and Motives for Financial Statement Fraud

Three Main Problem Areas

We will approach financial statement fraud looking at the following three broad areas:

1. Earnings manipulation
2. Earnings management
3. Balance-sheet manipulation

Financial statement fraud generally falls into one or more of the above categories.

10.2.1 Earnings Manipulation

Earnings manipulation is the direct alteration of accounting data for the purpose of fraudulently changing reported net income. For example, booking a sale that clearly does not meet the requirements for revenue recognition increases revenues. Conversely, capitalizing marketing costs as an asset, contrary to guidance in GAAP, decreases current period expenses. Notice also that both examples affect the balance sheet as well: recognizing fictitious sales would inflate accounts receivable; deferring marketing expenses creates some type of amortizable asset. Because the primary intent of these manipulations is, however, to increase earnings rather than create assets, these practices are classified as "Earnings Manipulation."

Motives for Earnings Manipulation

The motives for earnings manipulation usually stem from the need to report higher net income. Management compensation agreements, for instance, may require the achievement of some absolute level of net income or an increase in net income over some benchmark in order to trigger bonus payments. Pressure to increase "shareholder value" may provide another motive to create earnings increases. Because stocks are valued at some multiple of price to earnings, an increase in earnings usually increases share price even if the multiple stays constant. If earnings are growing rapidly, the multiple is more likely to expand.

Earnings manipulation may also help support the share price of a publicly traded company while management and insiders sell their holdings. Such a reprieve may be important if time restrictions prevented the granting or sale of those shares at an earlier date. Examples of stock granting or sale restrictions include the following:

1. Vesting provisions in employee stock ownership plans that postpone ownership
2. Stock option exercise restrictions that prevent managers from acquiring shares until specified dates or the occurrence of specific events
3. SEC Rule 144A restrictions that limit the number of shares that can be sold on U. S. securities exchanges on a given trading day
4. Income tax provisions that afford more favorable tax treatment to long-term capital gain on the disposition of shares that meet the holding-period requirements (the restriction being that the government would receive more of the sale proceeds if the gain from the disposition of the shares were classified as short-term capital gains)
5. Corporate control requirements that necessitate holding significant blocks of stock past some event such as an annual shareholders' meeting before they can be sold

Finally, earnings manipulation may help a company obtain or retain its listing on a stock exchange. The initial and continued listing requirements of many exchanges provide for some type of net income test. Although companies failing this test may qualify for initial or continued listing under other tests such as overall market capitalization, companies whose share prices have declined sharply in a weak market may find net income manipulation to be their only hope. Losing an exchange listing may relegate the company to the over-the-counter market where there are no requirements for the presence of a minimum number of market makers, that is, the securities firms that stand ready to buy or sell shares to maintain an orderly market in the company's stock. Without a minimum number of market makers, investors face the prospect of greatly reduced liquidity. A shareholder wishing to sell his or her shares risks having to wait a long time for a buyer to come into the market. Therefore, a listing on a recognized exchange that mandates a minimum number of market makers is an important benefit to a publicly traded company, a benefit that unscrupulous management may implement earnings manipulation to retain.

10.2.2 Earnings Management

A subtler variant of earnings manipulation is earnings management. Although both involve the manipulation of accounting data, the latter attempts to produce reported earnings that conform to outside expectations. Corporate managements are under more pressure today than ever before to increase "shareholder value," that is, the price of the stock. Superstar analysts raise performance expectations by generating earnings estimates that strongly influence stock prices. Management, fearing the precipitous decline that can result if analysts scale back their growth estimates, may believe that the company must *massage* its numbers to meet analysts' expectations.

In this environment, the moral issue of reporting earnings that truly measures the company's economic activity is a matter of management intent. The very nature of accrual accounting leaves open the possibility that management judgment even within GAAP may be colored by the intent to show the company in the best possible light. Accrual, deferral, and allocation procedures designed to permit the relation of revenues and expenses, gains, and losses across periods also allow management considerable leeway as to when to declare any monies are *earned*. When, within this process, does discretion become the intent to deceive? Within what limits should management be acting to permit investors to price the company's securities in the market? How much earnings *smoothing* actually misrepresents the trend of economic performance as opposed to the irregularities of cash flows? Earnings management is fraudulent if improper accounting is used to hide true company performance. Arthur Levitt, chairman of the SEC, expressed the Commission's concern about this subject in a speech in 1998.

> Flexibility in accounting allows it to keep pace with business innovations. Abuses such as earnings management occur when people exploit this pliancy. Trickery is employed to obscure actual financial volatility. This, in turn, masks the true consequences of management's decisions.[6]

In SEC Staff Accounting Bulletin (SAB) No. 99, (the full text is included at the end of this chapter), the SEC reviewed the U.S. accounting literature and presented the staff's findings on earnings management.

Failure to **Perform** *Punishes the Stock Price*

Within this range of discretion, the managements of publicly traded companies, especially growth and high-tech companies, have been under tremendous pressure to perform for the last two decades from both analysts and investors. Failure to report continued profit growth has resulted in dramatic punishment to the stock price even if the shortfall is by only a few cents per share. Even performances that are good by historical standards can cause a price decline if they are below analysts' expectations. This kind of market reaction has been an incentive for companies that are just meeting analysts' forecasts or even falling slightly below to show a modest increase in reported profit.

Companies reporting consistently rising earnings are rewarded with high price earnings (P/E) multiples. As the chain of good quarters extends, the multiple tends to increase and vice versa. P/E multiples are effectively inverted capitalization rates that have built-in assumptions for future discount rates applied to expected future cash flows. If earnings grow steadily from period to period, analysts are better able to predict future earnings. The market tends to reward a company having a steady growth record with a lower discount rate that reflects a lower level of uncertainty about future earnings. This lower discount rate then increases the present value of future earnings and thus makes the stock or claim on those earnings more valuable.

Managements Regularly Meet Analysts' Forecasts

Recent academic studies have shown the regularity with which managements meet analysts' forecasts quarter after quarter and the small number of shortfalls. Managements themselves can influence analysts' estimates through meetings and other contacts with the result that the whole earnings estimation process seems to be manipulated. It has also been observed that analysts with underwriting houses tend to make higher growth forecasts than independent analysts.

It is hard to resist the conclusion that managements are often driven to *massage* the earnings components. Their bonuses are tied to operational performance and their stock options are tied to stock price performance. In addition, their overall performance will determine accessibility of capital for their companies. A good earnings report can improve the terms of a security offering to the benefit of both the firm and its management. The fact that shares of firms making seasoned equity offerings under-perform during the years

---

[6] Arthur Levitt, *The "Numbers Game,"* a speech presented to the New York University Center for Law and Business, Sept. 28, 1998. Available at http://www.sec.gov/news/speeches/spch220.txt.

immediately following the offering suggests that accruals were maximized in the year of the offering and earnings were allowed to deteriorate immediately thereafter.

Discovery of earnings manipulation can lead to the dismissal of senior executives, law suits by shareholders and sharp declines in the price of the company's stock. Other consequences will be a decline in the number of analysts following the company and an increase in the number of short sellers.[7]

Four Main Kinds of Earnings Management

SEC Chairman Levitt focused on the following four main fraudulent practices used to enhance earnings.

Big Bath Restructuring Charges. Big bath restructuring charges are the large one-time charges associated with a restructuring. Management may take a *big bath* charge on the assumption that the company stock price will get pummeled whether the restructuring charge is large or small. Using that logic (which may be correct), management opts for the big charge by establishing large reserves for shutting down operations or shifting operations to other areas. If the reserve estimates are too big and actual expenses do not consume all the reserves, management can later reverse the unused portion back into income. As an added bonus, the reversal back to income may occur at a time when earnings need a boost because of disappointing current operating results. Hence, Chairman Levitt observed that overestimation can leave charges that are "miraculously reborn as income when estimates change or future earnings fall short."

Writeoffs. After one company acquires another, research and development (R&D) work performed in one or both of the companies may be redundant because of a change in corporate direction under the new management. For that reason, companies may write off some in-process R&D projects that have yet to be expensed because they do not fit into the new corporate plans. A number of companies, however, have taken advantage of the opportunity to write off substantial amounts of in-process R&D, by applying a principle similar to the big bath restructuring charge. Management believes that the company can take a large, one-time hit to earnings without further hurting its stock price when the financial community is already expecting some writeoffs because of the acquisition. By taking the writeoff at the time of the acquisition, these R&D expenses will not weigh on future earnings.

Cookie Jar Reserves. Fraudulent managers tend to cloak their deception in an accounting rule, although in reality the accounting rule is not properly applied or other accounting rules are broken. The use of loss reserves is a good example of the abuse of a GAAP principle in order to manage the final earnings figure. In a calendar quarter in which a company expects to out-perform market expectations, it might create a reserve for future losses on such items as long-term contracts to create the effect of lowering earnings closer to the market consensus forecast. Then, in a future quarter, after the company has predicted that it will not make enough income to meet market expectations, management can reverse out some of the reserves on the grounds that future contract losses no longer appear probable.

---

[7] For an excellent survey, discussion, and bibliography of the academic and practitioner literature on this broad topic, see Patricia M. Dechow and Douglas J. Skinner, "Earnings Management: Reconciling the Views of Accounting Academics, Practitioners and Regulators," *Accounting Horizons*, June 2000, pages 235–250.

On the surface and viewed in isolation, the creation and reversal of the loss reserves may appear unrelated to earnings expectations. GAAP provides for the booking of loss contingencies in Financial Accounting Standards Board (FASB) Statement of Financial Accounting Standards No. 5, *Accounting for Contingencies,* provided the loss contingencies are both quantifiable and probable. In reality, however, the possibility of losses on future contracts most likely existed prior to the establishment of the reserve and continued to exist after the reserve was reversed into income. The reserves then become an accounting artifice used by management to manage earnings to meet market expectations. Moreover, management violated GAAP, in this example, either by creating the reserve without justification or reversing the reserve without any change in the degree of risk that the loss would in fact occur. Such reserves are known as *cookie jar reserves* because management can reach into the cookie jar and pull them into income whenever the need arises.

Materiality. Underlying the discussion of financial statement fraud to this point is the assumption that the accounting manipulations cited are all material in that the manipulations significantly change the information presented in the financial statements. Much of the accounting literature contains provisions that except immaterial amounts from a given accounting standard. However, the evolution of the definition of materiality has introduced another element of judgment into determining whether or not there is fraud.

Fortunately, the SEC decided to weigh in on this matter when it issued SAB 99 (the full text is included at the end of this chapter), which helped clarify some of the key materiality concepts. One of those issues the SEC addressed head on was the use of quantitative materiality to waive accounting violations. A blind application of quantitative materiality essentially looks at the monetary amount of an accounting entry (or series of entries) that was indefensibly improper. If the amount were less than some arbitrary standard such as five percent of net income, neither management nor company auditors would insist on changing that entry even though it blatantly violated accounting standards. The SEC said that although quantitative standards may serve as a starting point for investigating potential accounting irregularities, relying exclusively on an arbitrary percentage to avoid application of appropriate accounting standards has no basis in accounting literature (or in U.S. securities laws).

The FASB in 1980 issued Statement of Financial Accounting Concepts No. 2, *Qualitative Characteristics of Accounting Information,* which addressed materiality as follows.

> The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.[8]

In other words, materiality is viewed from the standpoint of the reader of financial statements. If the correction of an erroneous accounting item would probably cause the reader to come to a conclusion different from the conclusion reached upon reading the uncorrected statement, then the item is material. Prior to the release of FASB Concepts Statement No. 2, the U.S. Supreme Court, in reviewing a securities case involving materiality issues, ruled that a fact is material if there is "a substantial likelihood that the . . . fact would have been viewed by the reasonable investor as having significantly altered the

[8] FASB Concepts Statement No. 2, *Qualitative Characteristics of Accounting Information,* paragraph 132.

'total mix' of information made available."[9] Therefore, both accounting literature and the U.S. Supreme Court look to the reader or user of the financial statements and ask whether it is probable or substantially likely that the reader would have come to a different conclusion. If the answer is *yes*, then the item in question is material.

10.2.3 Balance-Sheet Manipulation

In addition to the creation of fictitious accounts receivable and improper capitalized expenses as discussed above, management can also manipulate assets. The value of a company can be misrepresented by any of the following:

1. Recording as purchases certain transactions for which title has not passed
2. Using improperly extended depreciation of useful lives
3. Failing to write down or write off useless assets

Management may inflate inventory by failing to bring the correct amount into cost of sales, a practice that has the added fraudulent benefit of inflating gross profit and earnings as well. Finally, management may manipulate capitalized acquisition costs through improper purchase price accounting, a practice described in detail in Section 10.4.2, "Kinds of and Motives for Financial Statement Fraud," herein.

Management manipulates liabilities by failing to record amounts owed to others or by keeping debts off the books. Management can also attempt to classify liabilities, especially loans to shareholders, as equity.

The motives for balance-sheet manipulation usually relate to reporting requirements established by lenders and regulators who tend to focus more heavily on balance-sheet items. A bank loan covenant, for example, may require a certain amount of shareholders' equity, a maximum debt-to-equity ratio, and/or a minimum current ratio. If the borrowing company's balance-sheet accounts violate the loan covenants, the company may be in default under the terms of the loan and subject to accelerated repayment of the loan or be precluded from any future loan advances. To make matters worse, a publicly traded company probably would have to report to securities regulators that it was in default under its loan covenants and as a consequence, suffer a decline in its stock price. Similarly, companies in regulated industries such as insurance and banking must maintain certain amounts of capital to meet regulatory requirements. Failure to do so may result in sanctions or even closure by the regulators. Therefore, motives for balance-sheet manipulation, while perhaps being more case-specific than those discussed previously for earnings fraud, nonetheless pose a real threat to accounting integrity.

10.2.4 Reducing the Risk of Fraud in Closely Held Companies

Much of this chapter focuses on publicly traded companies for two reasons. First, information about frauds committed in these entities is readily available. Second, regulators have been in the forefront of both the detection and the reduction of risk of fraud in publicly traded companies. Closely held private companies, however, can equally well experience every type of fraud discussed here; only the motives and timing are slightly different. Although the management of closely held companies might not have to worry

---

[9] *TSC Industries v. Northway, Inc., 426 U.S. 438, 449 (1976).*

about securities analysts' expectations, outside shareholders may demand better earnings performance. These demands might lead management to employ any of the earnings manipulation schemes discussed above. Of course, if management bonuses are a function of increased earnings, there is a motive for earnings manipulation regardless of whether the company is publicly traded or not. If the outside investors are passive, the moment of performance assessment will most likely be the end of the fiscal year. Management of public companies, on the other hand, may feel pressure to hit targets quarterly when they have to report to regulators.

The need to value shares in a closely held company may also give rise to earnings management. If shares are being valued for sale or any other purpose, such as collateral for a bank loan to a major shareholder, earnings management may be employed to achieve the appearance of a steady rise in earnings. This misleading rise in earnings could induce an appraiser or stock valuations specialist to assign a higher growth rate to projected earnings. It is just as likely, however, that the appearance of consistently rising earnings could suggest the use of a lower firm-specific risk premium to calculate the present value of that projected earnings stream since earnings would appear to be less volatile. The end result of earnings management in a closely held company is thus similar to the effect of earnings management on the P/E multiple of publicly traded companies.

For a closely held company, reducing fraud in the financial statements starts with requiring that financials presented to the board of directors and to outsiders be in conformity with GAAP. The timing of cash flows in cash-basis accounting can lead to the manipulation of financial statements.[10] Accrual-basis accounting looks to economic events to determine whether a debt is incurred or whether revenue is earned; the time of the occurrence of those events may be quite different from when cash is paid or received. What limits the possibility for fraud in accrual-basis accounting is the reduced opportunity to hide a debt or record unearned revenue since the standards of recognition are more explicit than those for cash-basis accounting.

It is difficult for both publicly held and closely held companies to communicate with outsiders such as lenders and investors without producing GAAP-based financial statements. In a sense, GAAP is the common financial language of the United States because it contains a set of rules and standards developed and tested over many years that are known to readers of financial statements. Certain foreign firms whose shares are not traded on U.S. exchanges may use local accounting standards or International Accounting Standards (IAS) for domestic reporting but would find raising capital in the United States problematic without translating those statements into GAAP.[11]

Additional fraud reduction measures include the implementation of internal controls discussed in Section 1.3 of this handbook and promoting an ethical environment, as covered in Chapter 2. For middle-market firms,[12] meaning, those with annual revenues of $10 million or more, the findings of the COSO, discussed in Section 10.3.2, "Qualitative

---

[10] For that reason, U.S. tax laws generally require corporations to report on an accrual basis when gross receipts exceed an average of $5 million per year over the prior three tax years.

[11] Indeed, if a foreign firm raises capital through the U.S. securities markets, it is required to issue financial statements in conformity with GAAP.

[12] *Middle market* is a term used by bankers to segment their lending markets, and that term is used here because closely held firms frequently interact with banks on matters involving their financial statements.

Predictors," below, are especially applicable since research conducted for the COSO found that smaller companies were more susceptible to fraud.

The importance of financial statement fraud reduction measures increases directly with company size. For a very small company, fraudulent financial statements that slightly inflate earnings or assets could be used to secure a bank loan or small investment but little else. Steps taken to prevent fraud at that level should reflect the potential for damages resulting from such misstatement. For larger, middle-market companies or small companies fraudulently representing themselves as larger companies, potential damages are more serious; steps taken to reduce fraud should therefore be more visible and systematic. For example, a middle-market company should implement reviews of internal controls at least once a year by outside CPAs and more frequently by internal accounting staff. If budgets allow, a significant fraud-reduction measure would include hiring an internal auditor, who is a CPA, to assess the effectiveness of the controls of each business unit. Assessments of the adequacy of internal controls would help significantly with early fraud detection.

The reporting of irregularities to independent board members is one of the most important fraud-prevention measures available to closely held companies. The opening of such a formal reporting channel increases the likelihood that corrective action will be taken. Without such a reporting channel, management, even if not directly involved in a fraud, might be inclined to sweep the problem under the rug for fear of reprisal or embarrassment. If the closely held firm has no outside directors (see Section 10.3.2 for a discussion of the independence of outside directors), a significant step to reduce the risk of fraud would be the appointment of such director(s).

10.3 PREDICTORS OF FINANCIAL STATEMENT FRAUD

Warning Signs

Faced with the apparent pervasiveness of earnings and balance-sheet falsification, the problem for the CPA is to find any warning signs suggesting the risk of fraud may be present. A number of recent studies (to be discussed in more detail below) have suggested a group of indicators which, when taken together, give the generic profile of a company at risk of fraud.[13]

The most typical fraud company is not listed on any of the major public stock exchanges. It has assets below $100 million and is experiencing losses, barely breaking even or reporting a small profit. The *trend* of net income is *not* an indicator since fraud can be committed to hide losses or preserve profits. Internal audit controls are weak or nonexistent. This can be attributed in part to the total absence of an audit committee or the presence of a weak one made up of financially unsophisticated directors meeting as infrequently as only once a year. More than 50 percent of the board of directors are insiders or "gray" directors, meaning, members with a large equity ownership or family, business, or other connection to the company or its board members. Few directors are on the boards of other companies and, therefore, the level of general business experience on the fraud company's board is often quite low. Officers frequently hold incompatible positions such as chief executive

[13] This portrait is drawn from Dechow and Skinner, and Levitt cited above, and important reports issued recently by the New York Stock Exchange and the National Association of Securities Dealers (NYSE/NASD) and COSO to be cited and discussed in Section 10.3.2 below.

officer (CEO) and chief financial officer (CFO) simultaneously. Finally, there usually is a change of CPA for the fraud period.

10.3.1 Quantitative Predictors

Messod D. Beneish, an associate professor at the Kelley School of Business, Indiana University, has tried to develop quantitative fraud warning signs by analyzing a series of ratios that might be used as predictors when seen as a pattern of irregularity on the books of a given company.[14] This model would distinguish manipulated from unmanipulated earnings within the definition of earnings manipulation as a violation of GAAP. Beneish studied seventy-four companies identified as earnings manipulators by the SEC or the media for the period 1982 to 1992.

Characteristics of Sample and Control Companies

The typical manipulator in Beneish's study was a young, rapidly growing manufacturing company (see table 10.1). As a group, they were smaller in terms of assets or sales, less profitable, more leveraged and growing faster than Beneish's control (presumably nonmanipulating) companies but with similar market capitalizations. Companies with poor prospects were more likely to commit financial statement fraud. Earnings manipulation typically occurred by recording fictitious revenues or inventory, unearned or uncertain revenues, or capitalizing costs improperly.

TABLE 10.1 CHARACTERISTICS OF SAMPLE AND CONTROL COMPANIES FISCAL YEAR PRIOR TO PUBLIC DISCLOSURE (1982–1992)

	Manipulators		Non-Manipulators	
Characteristics	**Mean**	**Median**	**Mean**	**Median**
Size (millions)				
Total Assets	$467.33	$43.20	$1,140.37	$ 95.84
Sales	469.87	53.56	1,295.22	122.54
Market Value	323.72	74.90	813.35	64.59
Liquidity/Leverage				
Working Capital to Total Assets	0.26	0.28	0.30	0.31
Current Ratio	2.54	1.83	2.54	2.11
Total Debt to Total Assets	0.58	0.58	0.51	0.52
Profitability/Growth				
Return on Assets	–1%	3%	3%	5%
Sales Growth	58	34	13	9

[14] Messod D. Beneish, "The Detection of Earnings Manipulation," *Financial Analysts Journal* (24) September/October 1999, pages 24–36.

Ratio and Index Analysis

Beneish identified a group of financial statement variables that capture actual earnings manipulation or indicate the potential for manipulation. Of that group, the Quantitative Financial Statement Fraud Indicators (see table 10.2), which are described in the following sections, generate statistically meaningful results.

Days' Sales in Receivables Index. The days' sales in receivables index (DSRI) is the year-over-year comparison of the annual receivables/sales ratio taken as a ratio. This ratio like all the other ratios in this study should be 1:1. If receivables are beginning to become large in relation to sales, fraudulent sales practices may be being put into place. After allowing for external factors, such as a more liberal credit policy that could have resulted in increased sales, an exceptionally large increase in receivables relative to sales might suggest revenue manipulation.

Gross Margin Index. The gross margin index (GMI) is the year-over-year comparison of gross margins taken as a ratio. If the GMI is greater than one, gross margins have weakened. Since the year-over-year deterioration of the gross margin is one of the most important signals of worsening prospects for the company, a GMI of greater than 1 is a red flag that financial statement manipulation may be about to occur.

Asset Quality Index. Asset quality is the ratio of noncurrent assets exclusive of property, plant and equipment to total assets in any given year. The asset quality index (AQI) ratio measures the proportion of assets whose power to produce future earnings is less certain. The higher the proportion of these intangibles to total assets, the greater the risk to future earnings growth. The AQI is the year-over-year comparison of these annual figures taken as a ratio. An AQI greater than one indicates that more costs are being capitalized and thus deferred and the door has been left open to earnings manipulation.

Sales Growth Index. The sales growth index (SGI) is the year-over-year comparison of sales taken as a ratio. Mere sales growth does not necessarily imply manipulation. Nevertheless, if a young growth company is under pressure from analysts, underwriters, and banks to show continuing sales increases to support the stock price, the possibility of manipulation is definitely present. Any dramatic increase in the SGI should alert the CPA to possible problems.

Total Accruals to Total Assets. The total accruals to total assets (TATA) is the year-over-year comparison of total accruals and total assets taken as a ratio in which total accruals are defined as the change in working capital accounts other than cash less depreciation. The presence of higher accruals, that is, less cash, is likely to be associated with earnings manipulation.

TABLE 10.2 CALCULATION OF THE QUANTITATIVE FINANCIAL STATEMENT FRAUD INDICATORS*

Notation: Current-year income statement and balance-sheet items are indicated with a subscript *t* and prior year items have a *t-1* subscript. The change in account balances from one year end to the next year end is denoted by Δ.

Days' Sales in Receivables Index =

$$(\text{Accounts Receivable}_t / \text{Sales}_t) / (\text{Accounts Receivable}_{t-1} / \text{Sales}_{t-1})$$

Gross Margin Index =

$$[(\text{Sales}_{t-1} - \text{Cost of Sales}_{t-1}) / \text{Sales}_{t-1}] / [(\text{Sales}_t - \text{Cost of Sales}_t) / \text{Sales}_t]$$

Asset Quality Index =

$$\frac{1 - [(\text{Current Assets}_t + \text{Net Fixed Assets}_t) / \text{Total Assets}_t]}{1 - [(\text{Current Assets}_{t-1} + \text{Net Fixed Assets}_{t-1}) / \text{Total Assets}_{t-1}]}$$

Sales Growth Index =

$$\text{Sales}_t / \text{Sales}_{t-1}$$

Total Accruals to Total Assets =

$$\frac{\Delta\text{Working Capital} - \Delta\text{Cash} - \Delta\text{Current Taxes Payable} - \text{Depreciation and amortization}_t}{\text{Total Assets}_t}$$

[1] Adapted from Beneish, *The Detection of Earnings Manipulation*, Financial Analysts Journal, September/October, 1999.

Look for the Pattern

Because of the interconnectedness of income and balance-sheet accounts, no single ratio should be taken in isolation as an indicator of manipulation. It is the *pattern* that counts, both among the accounts of one reporting period and over several periods. The broader the pattern, the greater the likelihood of earnings manipulation. But care should be taken that unusual ratios cannot be accounted for by acquisitions, shifts in strategy, or changes such as improving economic conditions and other normal business events.

The findings indicate that manipulators (see table 10.3) exhibit certain financial-statement characteristics that are detectable and different from nonmanipulators. The year-over-year change in days' sales in receivables, for example, was about 3 percent for nonmanipulators but over 46 percent for manipulators. Manipulators showed an increase of about 42 percent in days' sales in receivables in sales over the average change for the nonmanipulator peer group. The other indexes demonstrate similar though smaller increases for manipulators over nonmanipulators. The TATA, however, was markedly different between the two groups. The TATA measure, which reflects noncash working capital to total assets, probably picked up the increases in receivables that typically accompany revenue manipulation.

TABLE 10.3 MEANS ANALYSIS OF MANIPULATORS AND NONMANIPULATORS IN THE ESTIMATION SAMPLE**

Characteristic Measures	Manipulators Mean	Nonmanipulators Mean	Difference	Manipulators Percent Increase over Nonmanipulators
DSRI	1.465	1.031	0.434	42.1%
GMI	1.193	1.014	0.179	17.7%
AQI	1.254	1.039	0.215	20.7%
SGI	1.607	1.134	0.473	41.7%
TATA	0.031	0.018	0.013	72.2%

**Adapted from data provided in Beneish.

These characteristic measures provide a quick and easy means of detecting the possibility of financial statement fraud. They are indicators and do not by themselves prove fraud. CPAs, however, are required to implement Statement of Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 316),[15] may want to consider including these characteristic measures in their financial statement analyses. Also, as an internal control, an internal auditor or controller could apply these measures when reviewing financial information from subsidiaries and divisions. An increase in any of the characteristic measures in the magnitude indicated in the above table should trigger additional inquiries. Such inquiries may very well head off an incipient fraudulent scheme.

[15] Chapter 1 of this handbook discusses the auditor's duty to detect fraud in detail.

10.3.2 Qualitative Predictors

Internal Work Environment and Corporate Governance

The board of directors is a group of persons elected by the shareholders to represent them at the highest level of corporate decision making and to monitor the work of management. A report published in 1999 for the NYSE and NASD by the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (BRC) says explicitly that "the board must perform active and independent oversight to be, as the law requires, a fiduciary for those who invest in the company."[16] The board must be committed to the principles of transparency and full disclosure and, one might add, to full compliance with GAAP and the regulations of the appropriate regulatory bodies. If the board understands its independent role, then it is likely the audit committee, a creature of the board, will also do its duty. Companies proven to be earnings manipulators tend to be those with no audit committee or a very weak and compromised one. About a quarter of all companies subject to SEC enforcement action did not have audit committees.

The report sees the role of the audit committee as follows.

> The committee's job is clearly one of oversight and monitoring, and in carrying out this job it acts in reliance on senior financial management and the outside auditors. A proper and well-functioning system exists, therefore, when the three main groups responsible for financial reporting—the full board including the audit committee, financial management including the internal auditors, and the outside auditors—form a "three-legged stool" that supports responsible financial disclosure and active and participatory oversight.

Characteristics of a Good Audit Committee

The BRC made numerous recommendations for the effective working of a good audit committee. Despite the fact that the BRC's mandate was to make recommendations for the conduct of audit committees of companies big enough to be listed on the NYSE or the National Association of Security Dealers and Quotation Analysts (NASDAQ), many of the principles would apply equally well to smaller, private companies.

The foundation of a good audit committee is the independence of its members. Recent studies have shown a direct correlation between audit committee independence and better monitoring and a lower incidence of financial statement fraud. The BRC defines independence as follows.

> Members of the audit committee shall be considered independent if they have no relationship to the corporation that may interfere with the exercise of their independence from management and the corporation. Examples of such relationships include:
>
> - A director being employed by the corporation or any of its affiliates for the current year or any of the past five years;

[16] Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees, 1999. Available at http://www.nyse.com/ and http://www.nasdaqnews.com/.

- A director accepting any compensation from the corporation or any of its affiliates other than compensation for board service or benefits under a tax-qualified retirement plan;
- A director being a member of the immediate family of an individual who is, or has been in any of the past five years, employed by the corporation or any of its affiliates as an executive officer;
- A director being a partner in, or a controlling shareholder or to which the corporation made, or from which the corporation received, payments that are or have been significant to the corporation or business organization in any of the past five years;
- A director being employed as an executive of another company where any of the corporation's executives serves on that company's compensation committee.

Building on this foundation of independence, the BRC recommends that for listed companies with capitalization in excess of $200 million, the audit committee should be composed of a minimum of three financially literate and entirely independent directors. The audit committee should have a charter approved by the full board describing its structure and responsibilities. The outside CPA should be accountable to the whole board of directors. The audit committee should be responsible for the selection of the outside CPA. The audit committee should have a formal written statement from the outside CPA describing all relationships between itself and the company. The audit committee should discuss with the outside CPA all aspects of the effectiveness or lack thereof of the company's accounting practices. If the board of directors is weak and the audit committee is weak or nonexistent, internal controls are likely to be deficient or lacking altogether.

COSO

The COSO, a voluntary private sector organization dedicated to improving the quality of financial reporting, in its recently published *Fraudulent Financial Reporting: 1987–1997—An Analysis of U.S. Public Companies* sought to identify and examine company and management characteristics in corporations involved in financial statement fraud.[17] The COSO examined about 200 cases from which it drew a number of generalized conclusions about the governance of fraud companies.

The presence and efficient functioning of internal controls is central to limiting the opportunities for fraud. Unfortunately, the small size of many companies makes them unable or unwilling to spend the money for proper controls or to pay for better trained and more experienced senior executives. These smaller companies are also unlikely to have strong audit committees capable of monitoring the nebulous but important matter of pressure on senior executives to report aggressively to meet investment community expectations or the numbers required to trigger bonuses. The CEO or CFO was involved in 83 percent of the reported fraud cases.

A strong audit committee is an essential element in fraud prevention. Among the fraud companies surveyed, 25 percent had no audit committee and among those that did, 65 percent of the directors were not certified in accounting or had held no accounting or

[17] http://www.coso.org/main.htm.

financial positions. At the fraud companies, the committee usually met only once a year. (A pliable, inexperienced, and inattentive board is often the creation of a domineering CEO. Given the fact that in 83 percent of the reported fraud cases the CEO or CFO was involved, the combination of a weak board and aggressive leaders could be an indicator of financial statement fraud.)

The COSO report confirmed the findings of the BRC mentioned above concerning the need for an independent board of directors. At the fraudulent companies, about 60 percent of the board members were insiders or "gray" directors, meaning, outsiders with some family, business, equity, or other tie to the company or its management. About 40 percent of the boards had no directors serving on the boards of other companies. Directors and officers owned about a third of the companies' stock while the CEO or president owned about 17 percent. In about 40 percent of the companies, there were family relationships among the directors and officers. About 20 percent showed officers holding incompatible positions such as CEO and CFO.

The average period during which fraud occurred was 23.7 months and often started with the misstatement of interim statements. Therefore, it is important to review the controls surrounding quarterly statement preparation. Because misstatements of accounts often occur near the period ends, internal controls relating to transaction cutoff and asset valuation should be tested.

The Boeing Company adopted recommendations from a previous COSO report entitled *Internal Control–Integrated Framework* and came up with a list of criteria to be used to establish an unsatisfactory rating.[18] The following sections describe those criteria.

Control Environment. The criteria for the control environment are the following.

- *Hard controls* are missing or inadequate.
- There are verified instances of breakdowns or *soft controls.*

Risk Assessment. The criteria for risk assessment are the following.

- Management has not predefined relevant objectives.
- Such objectives are incompatible with broader objectives.
- Management has not identified relevant risks to achieving its objectives.
- Management does not have a basis for determining which risks are most critical.
- Management has not ensured mitigation of critical operating risks.
- Audit tests detect key risks not previously contemplated by management.

Control Activities. The criteria for control activities are the following.

- Key control activities are not functioning as intended.
- Management's risks mitigation strategy is not adequately reflected within control activities.

[18] Dennis Applegate and Ted Wills, "Struggling to Incorporate the COSO Recommendations into Your Audit Process? Here's One Audit Shop's Winning Strategy," *Internal Auditor*, published by The Institute of Internal Auditors, December 1999, http://www.coso.org/Articles/audit_shop.htm.

Information and Communication. The criteria for information and communication are the following.

- Key metrics are not identified, collected, and communicated.
- Employees' misunderstanding of their control responsibilities is pervasive.
- Customer or supplier complaints and disputes are not resolved or remedial action is not undertaken in a timely manner.

Monitoring. Management has not established a means of determining the quality of the internal control system over time either through independent evaluations or ongoing, structured, and independent process checks.

Overall. The ratings of all components should be considered to determine whether controls provide reasonable assurance that management objectives will be achieved. Strength in the internal controls of one component may compensate for a control weakness in another.

Buffalo Chips Inc. Case Study

When the accounts receivable accountant tripped over a box on the Buffalo Chips loading dock in October 1997, she knew something was wrong at the company. From the packing slip she recognized a $250,000 order she had invoiced in the previous quarter. As it turned out, booking revenues before products were shipped was only one of the fraudulent account practices used at Buffalo Chips to deceive its CPAs and investors.

In 1979, Buffalo Chips was a small Silicon Valley startup with a promising patent for semiconductor chips but the company had burned through its venture capital without bringing a product to market. Soon after Jim Johnson, a former engineer with defense and electronic-component firms, took over the company for no salary but 20 percent of the stock, the company became cash positive and had sales of nearly $2 million. Jim soon acquired the rest of the company. Mel Leeds was brought aboard in the accounting department and quickly became CFO. Johnson and Leeds had different personalities but shared a taste for expensive homes, cars, and golf.

Johnson had built up sales in specialty resistors and capacitors assembled on silicon chips by trading on his old connections in defense and electronics. Now he was successful in winning contracts to supply components to major American companies. Production capacity was increased by taking the company public and purchasing a microchip manufacturing facility from another producer. By 1987, revenues topped $30 million and 215 people were on the payroll. As the company grew, management was under relentless pressure from analysts to expand the P/E multiple and raise the stock price with a string of quarterly earnings increases.

Johnson was an overbearing manager who insisted on making decisions down to the level of twenty-five-dollar purchases of office equipment. The turnover of senior management was high with the result that the average level of executive experience declined. As early as 1987, product ordered for subsequent quarters was being shipped to meet current revenue objectives. Phony packing documents were created and product was stored onsite in empty offices and offsite in garages and elsewhere. The external CPAs forced the company to restate 1989 earnings to correct "revenue and expense cutoff errors" and recommended Leeds be fired. Johnson kept him on, however, but changed Leeds' title and some of his responsibilities, then raised his salary. In 1992, a new president tried to correct the situation but without success. He resigned after five months. The new CFO, Mario Innocente, who had been unemployed for nearly a year before joining Buffalo, did not.

Johnson told the executive in 1993 he wanted to see double-digit revenue growth every quarter because he wanted to attract new capital from a prospective partner and could raise another $40 million through a secondary offering if the stock price rose from its current $11 to $20. In 1994, Banzai Alloys bought 10 percent of Buffalo, promised an infusion of $24 million, and agreed to sell Buffalo's products overseas. The stock price jumped to $21.25 per share and the value of Johnson's holdings increased to $40 million. Leeds sold some of his holdings and netted more than $500,000. In the meantime, company executives booked bogus sales to both real and fictitious companies, treated product returns as sales, and produced false financial reports to deceive CPAs, bankers, and their own board of directors. False annual reports and 10-Q and 10-K filings were signed off, and misleading information was given to analysts.

Accounts receivable was now bursting with phony sales. To cover up, Innocente prepared two accounts receivable reports, one for internal use and the other for the board and investment bankers. The internal report showed that 51 percent of receivables were actually current; the outside report showed 82.4 percent. Even when a board member questioned the peculiar fact that receivables exceeded quarterly revenues, he was fobbed off with the answer that the Asian distributors had 180 days to pay and thus their receivable could be booked as current. He did not know that Asian sales were booked to distributors who had an unconditional right of return, that is, the products were, in effect, shipped on consignment. Cash collections fell to 25 percent of the quarterly target.

With the books in such bad shape, a secondary offering was now out of the question since the financial statements for the first nine months of fiscal 1998 could not survive an audit. It was initially suggested that $3 million in uncollectable receivables be written off but, toward the end of the fourth quarter, the amount had ballooned to $8.3 million. In consultation with Leeds, the new CFO decided to allocate the writedowns to product returns and bad debts. The writeoff would be offset by recognizing revenues of $7 million from Banzai as nonproduct technology sales.

When the figures were published, analysts became suspicious of the $8.3 million and $7 million figures and began to ask questions about the accounting for receivables. The stock price dropped to $13 from $22 in one day, and several shareholders filed lawsuits. A press release from the board of directors explained the accounting irregularities and the stock continued its downward path to $6. Johnson, Leeds, and Innocente departed and new CPAs restated a $7.7-million profit as a $16.6-million loss. Johnson and Leeds were indicted on the criminal charges of fraud and insider trading and received sentences of thirty-six and thirty-two months, respectively, and had to pay fines of $100,000 each. Johnson had to surrender his 1.5 million shares of Buffalo Chips valued at about $2.5 million in restitution to shareholders.

Conclusion and Analysis. How did this happen? First of all, the company was led by Jim Johnson, an ambitious and overbearing CEO, who found a compliant CFO in Mel Leeds. This proved to be a potent mix of personalities. Johnson had indeed shown great drive and competence in turning the struggling startup company into a profitable concern under his leadership. But as the company grew and went public in order to expand, it came under the scrutiny of Wall Street analysts. Management was now under pressure to meet analysts' earnings expectations. It was also necessary to keep revenues and earnings up in order to attract a new partner and raise additional capital through a secondary offering. Unfortunately, real revenues and earnings could not support these ambitions.

As came out in court, the company concocted nearly a dozen revenue recognition schemes. These included recording revenue on the following:

1. Goods shipped in subsequent quarters
2. Goods shipped before the customer agreed to accept delivery
3. Goods shipped to customers without receiving an order (These sales were not reversed when the goods were returned.)
4. Shipments held at the freight forwarder or stored offsite, sometimes at the homes of employees (Company shipping staff had deals with the forwarders to sign off on the paperwork as if real deliveries had been made.)
5. Goods shipped to fictitious customers
6. Goods shipped to customers with unconditional rights of return, that is, goods were shipped on consignment and recorded as sales

This scheme was concealed by the creation of a false accounts receivable report for the board of directors and investment bankers. The bankers and the board were deceived by the explanation that the high levels of receivables reflected large shipments made at the end of a quarter. They were not told that a number of sales were to customers with unconditional rights of return. After the whole scheme collapsed, forensic CPAs discovered that Buffalo Chips had recorded $38 million in phony revenue.

The SEC later alleged the CPAs had recklessly failed to comply with generally accepted auditing standards (GAAS) and had exercised improper professional conduct in the audit of accounts receivable, inventory, and property. Accounts receivable were overstated by $10.6 million or 162 percent; inventory was overstated by $10.2 million or 197 percent; property was overstated by $3.0 million or 40 percent. When restated, accounts receivable reduced net income by $9.7 million, inventory reduced net income by $9.3 million, and property and equipment reduced net income by $2.7 million. The SEC alleged that the CPAs had failed to exercise appropriate professional skepticism, obtain competent evidential matter, or properly supervise audit personnel. For example, the CPAs did not examine the writeoff of one third of the accounts receivable balance, an act that should have signaled to the CPAs that a material misstatement was possible. The SEC eventually brought Rule 102(e) proceedings against the engagement partner and manager on Buffalo Chips' 1994 audit.

10.4 SPECIAL AREAS OF FINANCIAL STATEMENT FRAUD

Certain items on a firm's financial statements appear to be especially vulnerable to fraud. The following discussion highlights four major fraud-prone areas and the steps that can lead to early detection:

1. Failure to record loss contingencies and asset writeoffs
2. Manipulation of acquisition reserves
3. Cost shifting to improve current operating results
4. Recognizing fictitious revenue

The common thread running through all these areas is that detection requires *the CPA to look for something not present in the financial statements.* CPAs are accustomed to beginning with a trial balance listing of all accounts and determining the procedures necessary to complete the audit. An item that does not show up on that trial balance at all, however, may never come to the attention of the CPA. For instance, in order to detect a failure to book a loss reserve for a contingent liability, one must first discover the existence of the contingency. From an auditing perspective, in the case of a failure to record a loss contingency, there is no loss contingency balance to audit; the accounting entry simply does not exist. Similarly, using acquisition reserves to hide current period expenses means that the expense item or category is absent from the income statement and is buried in some balance-sheet account relating to a prior business combination.

Cost shifting, meaning the movement of expenses from one entity or period to another, is equally hard to find. If the CPA looks at the accounts for the one business as of a given date, he or she does not see expenses shunted over to another affiliate or to another time period. In the case of fictitious revenue, although the CPA does at least have income statement revenue accounts to examine, the presence of side letters with customers, for example, which grant those customers the right to return product, does not show up as a contingency or in the footnotes. In practice, a CPA is not likely to be told that side letters exist.

Clearly, these are the toughest kinds of financial statement fraud to detect. Nevertheless, for each fraud discussed above, there may be some warning signs the CPA should look for. Those red flags may be small in dollar amount but point to significant irregularities. The following discussion assumes that a certain subset of management has attempted to manipulate financial data and looks at these issues in the context of audit planning and execution to determine what additional steps a CPA could take that might lead to detection of the fraud.[19]

[19] If financial statement fraud is traceable to a significant number of senior managers, the auditor should consider taking additional steps. For internal CPAs, those steps would include discussions with legal counsel. Outside CPAs should consider issuing a qualified opinion or, more likely, resigning from the audit engagement altogether.

10.4.1 Failure to Record Loss Contingencies and Asset Writeoffs

Loss Contingencies

A loss contingency is defined in FASB Statement No. 5, *Accounting for Contingencies,* as "an existing condition, situation, or set of circumstances involving uncertainty as to possible … loss … to an enterprise that will ultimately be resolved when one or more future events occur or fail to occur."[20] FASB Statement No. 5 continues to state that the "[r]esolution of the uncertainty may confirm … the loss or impairment of an asset or the incurrence of a liability."[21]

FASB Statement No. 5 lists examples of loss contingencies that include the following:

1. Collectibility of receivables
2. Obligations related to product warranties and product defects
3. Risk of loss or damage of enterprise property
4. Threat of expropriation of assets
5. Pending or threatened litigation
6. Actual or possible claims and assessments
7. Guarantees of indebtedness of others
8. Agreements to repurchase receivables (or repurchase related property) that have been sold[22]

A firm is required to accrue a loss contingency when that contingency is both *probable* and *able to be estimated.* FASB Statement No. 5 states the following.

> An estimated loss from a loss contingency . . . shall be accrued by a charge to income if both of the following conditions are met:
>
> a. Information available prior to issuance of the financial statements indicates that it is probable that an asset had been impaired or a liability had been incurred at the date of the financial statements. It is implicit in this condition that it must be probable that one or more future events will occur confirming the fact of the loss.
> b. The amount of loss can be reasonably estimated.[23]
>
> A future event is probable if it is "likely to occur."[24]

Having set the ground rules, we can examine some specific examples in the following sections.

[20] FASB No. 5, *Accounting for Contingencies*, paragraph 1.
[21] *Ibid.*, paragraph 1.
[22] *Ibid.*, paragraph 4.
[23] *Ibid.*, paragraph 8.
[24] *Ibid.*, paagraph 3. Footnote disclosure of the loss contingency may be required if the future event is less than probable but is "reasonably possible;" if the chance of a future event is more than remote but less than likely, FASB Statement No. 5, paragraph10 requires disclosure in the financial statements of the nature of the contingency and an estimate of the potential loss.

Warranty and Product Claims Reserves. If a manufacturer experiences post-production problems with a certain product, it may begin to experience higher-than-expected returns or, more likely, claims for reimbursement or repair. Those claims may arise under a specific warranty, under product tort law or under consumer protection laws and regulations. At this point, the manufacturer must assess its overall cost exposure. It might be possible to estimate the extent of future claims as a percentage of production based on past experience with other products subject to similar problems. It might also be possible to estimate the cost of each claim, meaning, the cost of replacement or repair for each defective unit of product. If both an estimate of future claims and the cost of each claim are available, then the amount of loss can be reasonably estimated. FASB Statement No. 5 would require the booking of a loss contingency if the future claims were likely to occur. If, however, the manufacturer is already seeing large numbers of claims prior to or soon after the close of its financial reporting period,[25] it would be reasonable to assume that the likelihood of future claims is high and that a FASB Statement No. 5 reserve should be accrued with a charge to current earnings.

However, a manufacturer under pressure to achieve increased earnings may be very reluctant to accrue a warranty or product claims reserve. Management may take the position that the problem does not exist or cannot be quantified. But an alert CPA may detect certain red flags that indicate a problem does indeed exist and that its extent can be estimated. The red flags that indicate the existence of a contingency include the following:

1. The incidence of claims prior to the issuance of financial statements (discussed above)
2. Discussions with (and bills from) outside legal counsel
3. Internal correspondence within production and research staffs as to the need to address a critical problem with a product already on the market
4. Internal correspondence among department heads of production, R&D, general counsel, and senior management about post-production problems and product claims
5. External correspondence between the manufacturer and its customers about a given product concerning special price concessions or special return privileges
6. The incidence of special or overbudget freight charges to accommodate returns and/or the shipment of replacement product
7. Shifting of production schedules to manufacture replacement product
8. Halting manufacture of the product in question
9. Shifting of R&D staff away from planned research projects to applications engineering relating to redesign of existing products
10. Payments in sometimes seemingly immaterial amounts to customers on a regular basis over a period of weeks or months that indicate some arrangement to compensate for product defects

[25] Actually, FASB Statement No. 5 requires the assessment of contingencies arising from "information available *prior to issuance* of the financial statements" (emphasis added). Therefore, if claims relating to a prior period come to the attention of management during the preparation of financial statements for that prior period, management should consider booking a contingency as of the end of that period.

Once the existence of a loss contingency has been established or that it is likely to occur,[26] the next step is to determine whether the potential loss can be quantified. In this case, if the firm itself does not have actual experience with product claims or if that experience is not relevant to the product in question, the CPA should look outside the firm. Industry statistics on product liability and the incidence of claims are generally available from trade associations, government regulators, or independent research organizations. In the course of examining internal correspondence between department heads and within departments, however, the CPA will likely find some internal estimates of the extent of the problem. This becomes especially obvious if the correspondents are attempting to justify the allocation of additional staff and financial resources to combat the problem or to explain why production was shifted or halted. In short, the members of management not directly involved in manipulating the financial statements may speak quite frankly about the loss contingency.

Asset Writeoffs

An asset is not always worth its balance-sheet carrying value. Even if an appropriate depreciation schedule is established when the asset is acquired, over time the needs of the business enterprise may change. Because of rapid changes in engineering and materials applications, for example, manufacturing processes may need to be updated to remain economically competitive. The machinery used in the old processes may become obsolete well before the machines themselves actually wear out and are depreciated down to salvage value. Similarly, changes in customer demand may force a manufacturer to discontinue a certain product line and render useless equipment specially designed to build that product. Firms operating in highly competitive markets may lose business to a low-cost competitor and be forced to idle production lines. Occasionally, in order to obtain or retain a customer relationship, a firm may even deliberately quote a price for its products that does not cover the cost of acquiring and operating the equipment used to produce those products. In all these cases, management should assess whether the equipment carrying value is impaired, especially if there are no reasonable prospects of finding an alternative use for the equipment. In the event an impairment loss should be taken, however, management may fraudulently postpone that charge if it causes earnings to fall below a managed earnings target.[27]

To detect this fraud, the CPA must be particularly adept at seeing through management's pretensions to get to the facts. The best place to begin is to review fixed assets with divisional or production personnel. FASB Statement No. 121, *Accounting for the Impairment of Long-Lived Assets to Be Disposed Of*, the standard for impairment of long-lived assets, provides the following list of possible events that may give rise to an impairment:

1. A significant decrease in the market value of an asset
2. A significant change in the extent or manner in which an asset is used or a significant physical change in an asset

---

[26] For purposes of this discussion, we focus on failure to accrue a probable loss contingency. However, violations of GAAP (and securities laws if the company files with the SEC) may occur if the firm has a reasonably possible loss contingency, according to FASB Statement No. 5, paragraph 10, but fails to make the required disclosure of that contingency in its financial statements.

[27] In this section, we are discussing asset writeoffs in the course of operations. Acquisition-related writeoffs are discussed in the previous section entitled "Big Bath Restructuring Charges."

3. A significant adverse change in legal factors or in the business climate that could affect the value of an asset or an adverse action or assessment by a regulator
4. An accumulation of costs significantly in excess of the amount originally expected to acquire or construct an asset
5. A current period operating or cash flow loss combined with a history of operating or cash flow losses or a projection or forecast that demonstrates continuing losses associated with an asset used for the purpose of producing revenue[28]

The CPA may wish to draw questions for firm personnel from this list and look for evidence of changes in production and product demand to determine whether an asset is impaired.

Clearly, if equipment has been moved off the shop floor into storage, and there are no plans for future use of that equipment, an impairment loss is highly likely. The more difficult issues arise if equipment is still in use but profitability is less certain. Profitability is at issue if assets may be impaired because FASB Statement No. 121 states that "[i]f the sum of expected future cash flows (undiscounted and without interest charges) is less than the carrying amount of the asset, the entity shall recognize an impairment loss...."[29] Since most management reporting systems, however, measure profitability by product line or by customer, it is hard to imagine how a business could survive in today's competitive environment without this information. Indeed, the activity-based costing initiatives begun in the 1980s were a direct result of the need for management to understand a product's contribution to overall firm profitability. Although CPAs may not be accustomed to reviewing product line profitability reports, these reports source revenues to the costs to produce them and can answer directly whether a given production process has been historically profitable.

Historical data are the basis of management plans and profitability forecasts. If the CPA can obtain such forecasts directly from the personnel with line responsibility for production, those personnel might be inclined to render a more accurate forecast since they are unaware of management's earnings target. One should keep in mind that line managers may have an incentive to show as positive a picture as possible to avoid a shutdown of production. Also, line managers may receive hints or outright requests from management to produce an overly favorable forecast. In either case, however, if the forecasts are accompanied by written narratives, the narratives will generally list all the downside possibilities in order to provide political cover for the line manager should events not turn out as planned.[30] The CPA may be able to assess the reasonableness of the forecast given the known conditions at the time and the likelihood of those downside possibilities.

Proving fraud in a forecast is difficult because a forecast is by its very nature a best guess.[31] If that forecast, however, was based on facts known to be incorrect, such as a major customer's known unwillingness to buy the product, then the forecast was fraudulently constructed. A forecast may also become fraudulent if it is used at a later time to justify a

[28] FASB Statement 121, *Accounting for the Impairment of Long-Lived Assets and for Long-Lived Assets to Be Disposed Of*, paragragh 5.
[29] *Ibid.*, paragraph 6.
[30] If there are no narratives, the auditor can probably obtain a list of potential downside possibilities simply by asking the line managers.
[31] For a definition of financial forecast, see AICPA *Guide for Prospective Financial Statements*, §200.04.

management decision because management knows that significant facts have changed. For example, a forecast may accurately reflect that, at the time of preparation, there was a possibility that a certain major customer wanted to buy the product. If, however, by the balance-sheet date, management knows that the customer is not interested and there are no alternative buyers, it would be fraudulent to assert that the forecast is still accurate and then use it to justify not writing down the value of assets used to produce that product.

Another area of asset writeoff that can fall victim to fraud deals with investments in the nonpublicly traded securities of companies. Such securities are difficult to value because transaction prices are not publicly available. If the security held is stock and there have been substantial historical operating losses with little hope of future profitability (meaning, the decline in value is other than temporary), that stock may be impaired according to FASB Statement No. 115, *Accounting for Certain Investments in Debt and Equity Securities.* Likewise, FASB Statement No. 115 states that for debt:

> ... if it is possible that the investor will be unable to collect all amounts due according to the contractual terms of a debt security not impaired at acquisition, an other-than-temporary impairment shall be considered to have occurred. If the decline in fair value [*of any security*] is judged to be other than temporary, the cost basis of the individual security shall be written down to fair value as a new cost basis and the amount of the write-down shall be included in earnings (that is, accounted for as a realized loss).[32]

Without recent prices for the sale of stock and debt in a private company, the CPA might have to look at financial information from the investee company. The investor, if it holds a significant position in the investee, should have financial information on file (if not, this should be a red flag that something may be amiss). Those data would likely include results of operations that would give historical profitability. For future profit estimates, one should look to company forecasts and assess the validity of those forecasts based upon known relationships, if any, between the management of the investor and investee. If there exists common representation within management or on the boards of both companies, further inquiry may be necessary to determine the validity of any forecast. Losses over several past yearsmay be sufficient to establish impairment, as the following case study taken from a SEC Accounting and Auditing Enforcement Release (AAER) demonstrates.

Windpower Inc. Case Study

Windpower Inc., a small private company, began doing research in windmill production and technology in 1978 with a view to later commercial development. The following year, the same group of investors established Breezy Valley Energy Inc. and transferred Windpower's R&D work to Breezy Valley in 1980. Breezy Valley reimbursed Windpower $31,308 for work done to date and from then on Windpower lent Breezy Valley money for R&D. In fact, these loans formed the primary source of funds for Breezy Valley.

[32] FASB Statement No. 115, *Accounting for Certain Investments in Debt and Equity Securities*, paragraph 16.

According to Windpower's financial statements for the nine months ended March 31, 1981, loans outstanding to Breezy Valley at that date amounted to $108,434. By the end of the following fiscal year, the aggregate loans totaled $208,146, and by March 31, 1983, they reached $321,725. In Windpower's financial statements for 1981 and 1982, the loans are accounted for as a receivable; during fiscal 1983, this receivable was exchanged for Breezy Valley preferred stock.

In September 1983, Windpower filed a Form S-1 in connection with a proposed $4-million initial public offering. In this filing, Windpower's investment in Breezy Valley was carried as an asset valued at historical cost rather than written down as Breezy Valley's prospects dimmed. Windpower's investment as reported in its various forms, represented 62 percent, 77 percent, and 80 percent of total assets at the end of fiscal years 1981, 1982, and 1983, successively, while cumulative operating losses increased at Breezy Valley from $118,420 in fiscal 1981 to $265,542 in 1982 and reached $437,092 by the end of fiscal 1983. Revenues for Breezy Valley had declined to such a degree that it was bringing in only $1 for every $7 going out in expenses; future earnings prospects were unattractive because Breezy Valley seemed unable to market its products.

Conclusion and Analysis. On the grounds of its failure to write down its investment in Breezy Valley to net realizable value in accordance with GAAP, the SEC suspended the effectiveness of Windpower's registration statement for the $4-million public offering. Since this case predated the issuance of FASB Statement No. 115, the SEC looked to FASB Statement No. 5 and found that Windpower should have applied the provisions of FAS 5 which states in paragraph 8 that:

> An estimated loss from a loss contingency . . . shall be accrued by a charge to income if both the following conditions are met:
>
> a) Information available prior to issuance of the financial statements indicates that it is probable that an asset has been impaired or a liability has been incurred at the date of the financial statements. It is implicit in this condition that it must be probable that one or more future events will occur confirming the fact of the loss.
>
> b) The amount of the loss can be reasonably estimated.

Windpower's financial condition met the requirements of paragraph a) since the investment in Breezy Valley was impaired and recovery was unlikely because of the growing losses and limited prospects of generating sales. The requirements of paragraph b) were also met since the amount of the loss was exactly equal to the known aggregate amount of the loans. Clearly the impairment requirements of FASB Statement No. 115, if it had been in effect, were also met.

On the basis of this failure to take account of the reduced value of Windpower's investment and the slim prospects of recovery, the SEC instituted proceedings against Windpower's CPA and two of its partners for improperly certifying that Windpower's financial statements had been prepared according to GAAP and audited according to GAAS. The SEC accepted Offers of Settlement and Undertakings from the CPA and its two partners.

10.4.2 Manipulation of Acquisition Reserves

If one company acquires another using the purchase method of accounting for the transaction under Accounting Principles Board (APB) Opinion No. 16, *Business Combinations,* the purchase price paid is allocated to the assets of the acquired company using the fair value of those assets. Any excess of purchase price over the fair value of assets acquired is booked as goodwill. Liabilities can also be transferred or accrued; those liabilities assumed by the purchaser effectively increase the amount paid. If, as is usually the case, the cash portion of the purchase price covers the fair value of assets acquired, then liabilities assumed over and above the cash paid will increase goodwill.

One type of liability managers of an acquiring company may wish to set up are loss contingencies as provided under FASB Statement No. 5,[33] presumably for potential problems inherited or created when the target company is acquired. These loss contingencies or reserves, as they are more commonly known, typically increase the goodwill paid for the acquired company meaning, the entry establishing the loss contingency is a credit to a reserve liability and a debit to goodwill. That goodwill is then amortized into income, usually over a forty-year period. Examples would include reserves for warranties on discontinued products or reserves for bad debts that would no longer be serviced as the acquiring company consolidates operations of the target and closes or sells off unwanted segments. Management may also wish to set up severance reserves for employee layoffs. If those contingencies later materialize, the expense (debit) of performing the warranty work, writing off the debt, or paying severance is then taken to the reserve as a credit balance on the liability section of the balance sheet.

Most important, the expense of a reserved item does not run through the income statement. Instead, because setting up the reserve itself created or increased goodwill from the purchase transaction, amortization of the goodwill attributable to the reserve comes into the income statement but only a small portion, perhaps as little as one-fortieth, is expensed in a given year. Therefore, establishing the reserve allows management to avoid taking the entire expense into income in the current period and, by the amortization of goodwill, to spread that expense over a much longer future time.

Clearly, management has an incentive to reserve as much as possible when making acquisitions. Moreover, management does not need to attempt to set up all necessary reserves by the date of the acquisition; FASB Statement No. 38, *Accounting for Preacquisition Contingencies of Purchased Enterprises (an Amendment of APB Opinion No. 16),* provides for a twelve-month period after the acquisition date to adjust the purchase price. It is here that management actions need to be carefully reviewed. Without restrictions on the booking of reserves after an acquisition, the management of an acquiring company could constantly (and conveniently) create reserves to absorb current losses from an acquired company.

At some point, however, current management must take responsibility for current period results. The twelve-month cutoff provided in FASB Statement No. 38 is the outside limit;

---

[33] Other accounting literature discussing when and how contingencies can be incurred in connection with a business combination includes SEC SAB 100 and Emerging Issues Task Force (EITF) Issues Nos. 94-3, *Liability Recognition for Certain Employee Termination Benefits and Other Costs to Exit an Activity (Including Certain Costs Incurred in a Restructuring),* and 95-3, *Recognition of Liabilities in Connection with a Purchase Business Combination.*

the period for adjusting the purchase price should end when management "is no longer waiting for information that it has arranged to obtain and that is known to be available or obtainable"[34] at the time of the acquisition. Management crosses the line into fraud when it creates material purchase reserves for losses that were not foreseeable at the time of purchase, especially if management creates those reserves and adjusts the purchase price more than twelve months after the purchase date. Likewise, management also commits fraud when it uses reserves to absorb losses unrelated to the reasons for which the reserves were established.

Fabulous Deals Inc. Case Study

As a divisional controller was about to go into a budget meeting, the Deal Club corporate CFO and corporate controller handed him new numbers inflating his revenue estimates by $200 million. He had already stayed up past midnight designing fictitious accounts under the corporate controller's instructions to create numbers that met analysts' estimates.

But this scene was not to be enacted until twenty years after Bill Battler, a wealthy Harvard MBA, had taken over Deal Club, a small discount-shopping club, in 1976 and went public with it in 1983 at 25 times sales despite losing $2.5 million on only $4 million in revenues the previous year. By 1997, Battler had built it into a business reporting $2.3 billion in annual revenues. Battler had grown the business by persuading large credit card companies to promote the club to their cardholders. He also founded or acquired more than a dozen similar clubs in the travel and other industries and brought them under Deal Club's umbrella. Proud of a reported 70 percent membership renewal rate that provided what Battler called an "annuity-like" stream of predictable earnings, he saw the stock move to the $25 area with a P/E of about 30.

Enter Carl Charise. A former tax lawyer, Charise founded Fabulous Franchises Inc. in 1990 and went public with it in 1992 at $4 a share. The company had the franchise rights to a number of hotel chains with a total of 500,000 rooms, real estate brokerages, rental cars, vacation time-sharing, and other businesses. Fabulous Franchises made money by charging a franchise fee and taking a percentage of earnings from its operators. Earnings were growing at an annual rate in excess of 60 percent because of Charise's good management and aggressive acquisition policy. The stock price hit a record $79 in 1996 creating a return of 2,000 percent since going public. In addition to an office at company headquarters in North Carolina, he kept an office in Manhattan from which he constantly wooed Wall Street analysts with the Fabulous Franchises story.

As each company grew bigger, growth opportunities became fewer. Battler and Charise began telling the analysts to lower expectations since both companies needed bigger and bigger acquisitions which were becoming harder and harder to find. In January 1997, Battler approached Charise proposing that Deal Club take

---

[34] FASB Statement No. 38, *Accounting for Preacquisition Contingencies of Purchased Enterprises (an amendment of APB Opinion No. 16),* paragraph 4.b.

over Fabulous Franchises. In the following months, discussions turned from acquisition by Deal Club to a merger of equals.

Superficially, the two companies seemed to make likely merger partners. The millions of well-to-do customers passing through Fabulous Franchises' operations were a natural market for Deal Club memberships and would create a new profit center. The merger would utilize the synergy of Fabulous Franchises' strong earnings and Deal Club's high multiple to add billions to market capitalization.

Trouble in Paradise began, however, when the two conflicting corporate cultures started to take a better look at each other. Bill Battler proved to be an absentee visionary and the company ran itself in a casual manner that sometimes slipped into carelessness. Divisions were left to run things their own way. Accounting systems were unsophisticated; financial reporting was slack; and there appears to have been little long-term planning. These practices were defended as entrepreneurial and had, indeed, unarguably produced a business with $2-billion-a-year in sales.

Carl Charise, on the other hand, was not only extremely charming to Wall Street, but also a very competent CEO who ran a tight ship. When his people demanded detailed nonpublic information including hard numbers, Deal Club executives backed off. In fact, the Deal Club president instead of producing numbers for the new management team produced one for himself, namely, a $25-million negotiated payout if he were not made Chief Operating Officer of the merged company after two years. The whole situation made Fabulous Franchises nervous but Deal Club's outside CPAs, gave assurances that the books were in excellent condition. Nevertheless, in the midst of all this prickliness, Deal Club kept delivering spectacular quarterly earnings. Fabulous Franchises executives could not confirm anything for themselves, however, and remained apprehensive.

After the two companies closed the merger under the name Fabulous Deals Inc. in late 1997, more unusual behavior began to surface at Deal Club. Bill Battler insisted that the old Deal Club remain financially autonomous and that CFO Haggis McMann and controller Patricia Candel remain in place. Deal Club's divisional controllers would not report to the merged company's chief accounting officer but to McMann and Candel, who would consolidate results before passing them on. This arrangement was reluctantly agreed to but financial reports continued to come in slowly and Fabulous Deals risked missing the 10-K filing deadline with the SEC. In the face of this problem and Charise's threats to take the matter to the board, Battler agreed to remove McMann and Candel from the process.

More peculiar matters began to come to light when the new chief accounting officer met with McMann, Candel, and others about the new reporting system. The former president of Deal Club asked him how to move $165 million from merger reserves into income "creatively" for fiscal 1998. It was also revealed that earnings had actually been increased by $100 million using this approach in 1997. When Charise heard this news, he was afraid he would have to restate earnings with all that implied for the stock price which he had so assiduously worked to support through his good relations with Wall Street. Former Deal Club executives tried to explain the matter away and the outside CPAs assured Charise that restatement would not be necessary.

The biggest bombshell, however, exploded a few weeks later at a routine budget meeting when two middle-level Deal Club executives revealed that Deal Club's growth story was a complete fiction and that the numbers had all been fabricated. The story, as it came out that day and over the next few weeks, showed that under instructions from McMann and Candel, more than 20 controllers at 17 of Deal Club's 22 divisions had committed fraud by creating $511 million in phony pretax income that translated into a one-third increase in earnings for the three years ended fiscal 1997. The fraud had grown each year until 1997 net income was 61 percent fiction. As the former Deal Club executives told the story, McMann and Candel had said the bogus numbers were necessary to meet analysts' forecasts.

When Charise publicly announced that Deal Club's 1997 earnings were being restated downward by $115 million, Fabulous Deals' stock price plunged to $19 from $36 to reduce market capitalization by $14 billion. At 108 million shares traded, the volume was the largest one-day turnover up to that time for any stock in NYSE history. Three shareholder law suits had been filed by the end of the day and about 70 more followed. By the time the stock price finally bottomed at $7.50, more than $29 billion in market capitalization had been vaporized.

Conclusion and Analysis. The fraud seems to have been driven by the perception of McMann, Candel, and others that meeting analysts' expectations and maintaining the upward momentum of the P/E and stock price were more important than accepting the ups and downs, the good years and bad, of business and all that that implied for the stock price. Externally perceived performance became more important than reality. The question of the degree of Bill Battler's involvement remains open.

The fraud was only able to go on as long as it did because of the failure of the CPA firm to detect the sizeable accounting irregularities. In the first three quarters of 1995, 1996, and 1997, the unaudited financial statements were doctored by adjusting revenues upward and expenses downward at the largest Deal Club subsidiary. These adjustments were $31 million, $87 million, and $176 million respectively. If the CPAs had looked at these interim statements, they would have seen a pattern of unsubstantiated changes to income and expense items. At year-end, before the CPA firm arrived to do the audit, these irregularities were reversed and the fictitious earnings replaced by earnings converted from cookie-jar reserves. The CPAs were so lax in their work that they failed to question this use of reserves. They even allowed a $25-million transfer from reserves to be classified as "immaterial." Acquisition reserves were even used to pay for $597,000 in expenses requested by Bill Battle for the operation of his private plane in years *prior to* the acquisition. These expenses, assuming they were properly reimbursable, should have been classified as operating costs.

This failure is even more troubling because the CPAs had had the Deal Club account for years and McMann, Candel, and others were former employees of the CPA firm. Bill Battle had even fought any change in CPAs after the merger. The CPA firm paid $335 million to settle a shareholder class action suit and is embroiled in other suits involving Fabulous Deals and Bill Battle. Fabulous Deals has agreed to pay $2.85 billion in class action settlements.

10.4.3 Cost Shifting Among Affiliates

If management desires to improve earnings fraudulently, it can remove expenses from the current period income statement to make operations appear more profitable. Expenses incurred by a firm can be shifted in the following two different ways:

1. Moved to the balance sheet to be brought onto the income statement at a future period
2. Moved to the income statement of another related entity to remove the cost altogether

Shift to the Balance Sheet

The matching principle, which states that the timing of expenses should be related to the timing of revenues,[35] restricts the first shifting method. Under this principle, if the cost was incurred to earn revenue in the current period, as a general rule, the cost should be charged to that revenue in the current period. There are some expenses that offer the prospect of providing benefits to future periods and management may attempt to justify capitalizing then amortizing them into income over future periods. This practice, however, may run afoul of specific accounting guidance and, if management intentionally ignores this guidance, it will create fraudulent financial statements. For example, to meet earnings projections, management may begin capitalizing the salaries of marketing personnel on the argument that the work they performed will benefit future-period sales.

Although there may be some conceptual merit to the argument, capitalizing sales personnel salaries runs directly counter to an example contained in FASB Concepts Statement No. 6, *Elements of Financial Statements (a replacement of FASB Concepts Statement No 3—incorporating an amendment of FASB Concepts Statement No. 2)*, paragraph 148 because it is difficult to determine the amount and length of time of future benefits.[36] Implementing the principle of conservatism, FASB Concepts Statement No. 6 states that such expenditures are "recognized as expenses in the period in which they are incurred because the period to which they otherwise relate is indeterminable or not worth the effort to determine."[37] Finally, even if capitalization is justified, the manipulation of financial statements may also occur if management switches from currently expensing costs to capitalizing them without proper disclosure. Failure to disclose may cause readers of financial statements to believe that profits have improved in the year of the policy change compared to previous periods when, in reality, the improved operating results may be solely attributable to shifting expenses to the balance sheet.

The Asset Quality Index, described in Section 10.3.2., "Quantitative Predictors," above, is one of the early warning signs of this type of manipulation. This index looks at the percentage of noncurrent assets to total assets for the current year over the previous year. If the index is greater than one, management has increased the percentage of noncurrent to

---

[35] See FASB Concepts Statement No. 6, *Elements of Financial Statements (a replacement of FASB Concepts Statement No. 3—incorporating an amendment of FASB Concepts Statement No. 2)*, paragraphs 145–149, for a summary of the issues regarding expense recognition.

[36] There is an exception that allows capitalization of sales commissions paid to agents selling insurance policies under FASB Statement No. 60, *Accounting and Reporting by Insurance Enterprises,* paragraph 28, *et seq.* In the case of insurance sales, though, actuaries are able to establish estimates of how long those policies will remain in force and thereby generate premium income to the insurance carrier. Those estimates then provide a reasonable basis for amortizing the commissions and other acquisition costs over future periods.

[37] FASB Concepts Statement No. 6, paragraph 148.

total assets. This type of behavior is frequently associated with the sale of stock, especially during the period leading up to seasoned equity offerings for a company whose stock is already publicly traded. (A seasoned equity offering consists of the sale of new, additional shares by a public company.) A survey of academic research also found that management frequently got away with this type of manipulation, as described in the following excerpt.

> Two recent studies provide evidence that managers manage earnings at the time of seasoned equity offerings (Rangan 1998; Teoh et al. 1998). It is well known that shares of firms that make seasoned equity offerings (SEOs) underperform the market in the years following the offering. These two papers show that: (1) reported earnings of firms that make SEOs are unusually high at the time of the SEO; (2) these high reported earnings are attributable to unusually high accruals (including "discretionary" accruals); (3) these firms' earnings performance is unusually poor in the years following the SEO; (4) there is a strong association between the extent of earnings management and subsequent stock price performance—shares of firms with the highest accruals at the time of the SEO tend to perform worse in the years after the SEO than shares of other firms. This evidence is consistent with the view that investors do not "see through" earnings management at the time of the SEO. Rather, as time passes after the SEO and the earnings management becomes apparent through subsequent earnings disappointments, the overpricing reverses and these stocks underperform the market[38].

Clearly, the incentive is to create a short-term illusion of higher profits to sell stock at an inflated price.

Shift to Related Entity

Sometimes fraudsters can deceive by moving costs from one entity to another under common control. This is useful to the fraudsters in situations in which investors or analysts are looking intently at the performance of a certain business segment and management wants to show rising earnings in that segment to give the illusion of significant future growth. A scenario similar to this played out in the W.R. Grace case,[39] although there management also used reserves as the tool to shift expenses (as per the discussion in the preceding subsection entitled "Cookie Jar Reserves"). In June 1999, the SEC brought a managed earnings case against Grace for manipulating the reported earnings of its primary health care subsidiary, National Medical Care, Inc. Management had established reserves for unanticipated health care reimbursements and used those reserves in subsequent periods to reduce expenses and show a steady growth rate in its health care subsidiary. However, there were no liabilities to justify the reserves, which consequently were not in conformity with GAAP. Fraudsters may also want to improve a subsidiary's earnings to dress it up for sale by shifting costs to the parent or to affiliates and by using reserves, as in the Grace example.

---

[38] Dechow and Skinner, *op. cit.*

[39] *In the Matter of W.R. Grace & Co.,* AAER No. 1140, June 30, 1999. This case also raised materiality issues in that the manipulation of subsidiary earnings was less than a rule-of-thumb threshold of 5 percent of consolidated Grace earnings. But since the SEC found that management placed increased importance on the subsidiary's earnings, the SEC determined that the manipulation was material.

Another example of cost shifting was the Livent case.[40] Livent, Inc. was a Canadian theater company that produced a number of successful Broadway shows including *Phantom of the Opera*, *Showboat*, and *Ragtime*. In January 1999, the SEC brought enforcement proceedings against nine former employees of Livent for their involvement in a scheme to inflate income by falsifying expenses among other things. This scheme operated from 1990 through 1998. The following were the three areas of expense manipulation.

1. Livent transferred preproduction costs for the shows to fixed assets, such as set construction.
2. Livent removed certain expenses and related liabilities from the general ledger.
3. Livent transferred costs from one show currently running to another show that had not yet opened.

Livent shows that this type of cost shifting is especially hard to detect. Livent, however, succeeded in its deception for eight years. Business downturns usually bring these schemes to the surface because, if the company overall is suffering, there is no place to hide the additional costs.

To try to detect cost shifting before a downturn, CPAs would be well served to look for credits appearing in expense accounts. Such credits may indicate that the entity incurring the cost accrued the expenses on its books first as debits and then transferred the expenses out with offsetting credits. It is not safe, however, to assume that the subsidiary incurring the expense initially recorded it as such. There may be a special reserve or liability account on the balance sheet set up to record the initial debits with the transfer credits appearing later. As the expenses are being booked, significant debit balances in the liability account will grow until the transfer is made. Such debit balances in a liability account should stand out. Also, if the transfers take place over time, there is likely to be some correspondence spelling out the procedures, especially if the initial debit is to an unusual account such as a liability reserve.

10.4.4 Recognizing Fictitious Revenues

The COSO report found that more than half the financial reporting frauds in the period 1987 to 1997 were attributable to overstating revenue. Revenue recognition issues have occupied the accounting profession for many years as well. In 1984, the FASB issued FASB Concepts Statement No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises.* That statement set out the following two basic requirements for recognizing revenue.

a. *Realized or realizable.* Revenues and gains generally are not recognized until realized or realizable. Revenues and gains are realized when products (goods or services), merchandise or other assets are exchanged for cash or claims to cash. Revenues and gains are realizable when related assets received or held are readily convertible to known amounts of cash or claims to cash. Readily convertible assets have (i) interchangeable (fungible) units and (ii) quoted prices available in an active market that can rapidly absorb the quantity held by the entity without significantly affecting the price.

[40] *In the matter of Livent, Inc.*, AAER No. 1095, January 13, 1999.

b. *Earned.* Revenues are not recognized until earned. An entity's revenue-earning activities involve delivering or producing goods, rendering services, or other activities that constitute its ongoing major or central operations, and revenues are considered to have been earned when the entity has substantially accomplished what it must do to be entitled to the benefits represented by the revenues....[41]

The staff of the SEC identified a long list of additional accounting pronouncements that address revenue recognition, including the following:

- FASB Statement No. 13, *Accounting for Leases*
- FASB Statement No. 45, *Accounting for Franchise Fee Revenue*
- FASB Statement No. 48, *Revenue Recognition When Right of Return Exists*
- FASB Statement No. 49, *Accounting for Product Financing Arrangements*
- FASB Statement No. 50, *Financial Reporting in the Record and Music Industry*
- FASB Statement No. 51, *Financial Reporting by Cable Television Companies*
- FASB Statement No. 66, *Accounting for Sales of Real Estate*
- APB Opinion 10, *Omnibus Opinion—1966*
- Accounting Research Bulletin (ARB) Nos. 43 and 45, *Long-Term Construction-Type Contracts*
- American Institute of Certified Public Accountants (AICPA) Statements of Position (SOP) No. 81-1, *Accounting for Performance of Construction-Type and Certain Production-Type Contracts*
- SOP No. 97-2, *Software Revenue Recognition*
- Emerging Issues Task Force (EITF) Issue No. 88-18, *Sales of Future Revenues*
- EITF Issue No. 91-9, *Revenue and Expense Recognition for Freight Services in Process*
- EITF Issue No. 95-1, *Revenue Recognition on Sales with a Guaranteed Minimum Resale Value*
- EITF Issue No. 95-4, *Revenue Recognition on Equipment Sold and Subsequently Repurchased Subject to an Operating Lease*[42]

In SAB 101, the SEC set out its interpretation of the above literature and concluded the following.

> The staff believes that revenue generally is realized or realizable and earned when all of the following criteria are met:
>
> a. Persuasive evidence of an arrangement exists
> b. Delivery has occurred or services have been rendered
> c. The seller's price to the buyer is fixed or determinable
> d. Collectibility is reasonably assured.[43]

---

[41] FASB Concepts Statement No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises,* paragraph 83 (footnotes omitted).
[42] SEC SAB 101, Topic 13, A.1.
[43] *Ibid.* Footnotes have been omitted.

With regard to a fixed or determinable selling price, the SEC staff amplified its position by looking to SOP 97-2 which defines a *fixed fee* as a "fee required to be paid at a set amount that is not subject to refund or adjustment."[44] Even though SOP 97-2 addresses software revenue recognition, the staff thought that the requirement of not being subject to refund or adjustment was applicable to all transactions. If the buyer retains a right to a refund of the purchase price, then collectibility *cannot* be assured. Indeed, it would be difficult to meet the FASB Concepts Statement No. 5 realization test if the cash or other payment tendered was subject to refund at the buyer's discretion. Yet refund arrangements are a common area for revenue recognition fraud. (For an example, see the case study entitled "Datatronix, Inc. Case Study," that follows this section.)

If company management wishes to inflate revenues by booking fictitious sales, in all likelihood, one or more of the SEC's conditions will have been violated. These conditions are described in the following sections.

Lack of an Agreement

As the reporting quarter draws to an end, companies straining to achieve a revenue target face pressure to close sales by the last day. That pressure may lead to the fraudulent booking of premature or nonexistent sales. In the rush to close transactions by a certain date, sales personnel may represent to management that there is an oral agreement with a customer when, in fact, there is none. For this reason, the SEC standard requires "persuasive evidence," which generally means some written documentation from either the buyer or a third party such as a purchasing agent. If a company requires a written agreement in order to credit a salesperson with a sale, the agreement might be held up, perhaps under review in the buyer's legal department, at the end of the quarter. The salesperson may then represent (perhaps accurately) that the buyer's purchasing decision maker has signed off on the sale; without a signed contract, however, recognition of the sale violates the company policy. Such a policy is put in place to assure the company conforms to GAAP. Violating that policy causes a GAAP violation if, in footnotes to the financial statements or elsewhere, management represents that sales are not recognized without a written agreement.[45] Such a violation might also point to an internal control issue for the CPAs to consider.

Good sales cutoff procedures can generally detect lack of proper agreements; but if written agreements are fabricated, detection is much more difficult. Random sampling of orders booked as revenue near the end of a quarter should provide a list of customers to call to verify that documents are authentic. For a document fabrication scheme to succeed over several quarters or years, however, the fabricated agreements must be replaced by authentic agreements and real sales or there will be significant reversals of prior period sales. Therefore, CPAs can compare, perhaps on a random basis, contracts on file at the end of a given reporting period with contracts on file for the same transaction at a later period of time. If the original (fake) contract has been switched, there probably was an attempt at

---

[44] AICPA Statement of Position 97-2, paragraph 8.

[45] See SAB 101, Question 1. The hypothetical posed in the SAB actually stated the normal and customary business practice was to obtain written agreements and did not mention the existence of a company policy to obtain written agreements. The staff's position was that companies could not book as revenue sales lacking written agreements when the normal and customary business practice for the industry was to obtain written agreements.

fabrication. Conversely, if the authentic document does not appear, the sale may never have been completed, in which case there would be a reversal in the subsequent period. Numerous instances of such reversals would point to revenue recognition problems.

Nondelivery

What constitutes delivery varies from industry to industry but generally occurs when title and risk of loss pass to the buyer. Delivery of some products require shipping documents that provide a paper trail that can be audited. Delivery of products such as software, though, may occur over the Internet at near instantaneous speed. Nevertheless, there should be some documentation or electronic receipt verification.

Attempts at achieving fraudulent deliveries usually involve some person or entity willing to hold the product until such time as its sale can be arranged. As part of the fraud scheme, the recipient executes documents or e-mails that appear to confirm delivery. This recipient is sometimes part of the scheme or can be a customer who inadvertently accepts delivery before consummating the sale. The latter may be easier to detect because customers receiving products before they are wanted tend to complain to company management. The third-party recipients who park goods temporarily may be harder to detect but usually require some payment for their services. Payment may come in the form of above-average discounts if the third parties resell the products over future periods, or there may be special terms allowing for product returns. An analysis of average product selling prices may point to one customer who stands out from the rest by receiving better deals. If returns from a given customer are abnormally high, that fact may also indicate special arrangements, especially if the returns occur in a later reporting period. If one customer receives such favorable treatment, the CPA should make additional inquiries as to why. In addition, delivery schemes involving resellers typically become more apparent if other resellers cannot sell the product as expected because of a change in market conditions. If a reseller is still taking substantial deliveries of product after many others are experiencing sales declines, the CPA should attempt to understand why that reseller's channels of distribution are clear while others are blocked.

No Fixed Price

Sometimes prices are difficult to determine, particularly if the product is to be combined with other products before being sold to an end user. Such sales may involve a royalty payment that is a function of the selling price. It would be inappropriate to book anticipated future royalties as current revenues until the amount of those royalties becomes fixed upon ultimate sale. Minimum royalties, however, may be booked when they become due. Fraud occurs when royalties are recognized on fictitious or anticipated ultimate sales. Such royalty arrangements, however, typically require the royalty payor to report to the royalty recipient the quantity of ultimate sales on a periodic (usually quarterly) basis. This permits an accounting of the final sales that can be used to verify reported royalty income.

The more deceptive form of fraud used to circumvent the fixed price requirement is the clandestine use of side letters or arrangements that allow for refunds or discounts at the buyer's option or in certain circumstances. Under tight market conditions or perhaps because the product is new and untested, it may be necessary to use these side letters to make a sale. The most likely candidates for this type of fraud are sales personnel with some discretion and authority such as divisional managers and above. Implementation of such a scheme requires their authority to alter records or invent excuses should the buyer exercise his rights under the side agreement. As a general rule, side letters are the result of some type of internal control failure when the divisional manager is able to effect economic outcomes and alter accounting records. These side letters are quite hard to detect because the buyer usually realizes he is receiving a special deal and does not want to publicize it. Of course, the fraudsters in the selling company will attempt to keep such agreements secret.

These schemes must come to the surface if the buyer exercises his rights under the agreement. A more senior member of management is usually involved to cover up the refund with a fabricated reason or another transaction. Nevertheless, there is usually some documentation of the refund if corporate controls are in place. The CPA who suspects the existence of side letters can certainly look for refunds and discounts that are out of the ordinary. Keep in mind that the customer probably demanded the right to obtain a refund or discount in the course of negotiations for the sale. To catch the existence of side letters before refund demands are made, a suspicious CPA may review sales files for correspondence, notes, or other evidence of such demands from the prospective customer. If the products involved requires personnel such as engineers to install the product, those personnel not reporting to the fraudsters may know details of the side agreement but innocently believe there is no issue to report to senior management. It is also likely that if fraudsters used side letters with one customer, there might be side letters with other customers as well.

Receivables Are Not Collectible

Financially weak firms may not pay their bills. To prevent sales to firms in poor financial condition, some type of customer-approval process independent of the sales function needs to be in place to assess customer health, especially if the customer is placing large orders. This review function should be integrated with the approval process for customer refunds and discounts to prevent the implementation of side letters, which also affect collectiblity, as discussed above. From a CPA's point of view, an unusual concentration of orders from small or distressed customers, particularly near the end of a reporting period or a sales campaign, should raise concerns.

Datatronix Inc. A Case Study

Datatronix is a multinational database software company with shares traded over the counter. The company described itself in its press releases and advertising literature as the fastest growing company in the database software industry. In reality, the company was showing increased revenues and earnings by using a wide range of fraudulent accounting practices to produce the numbers on its own financial statements as well as those filed with the SEC. For the fiscal years 1994 through1996 and for the first quarter of fiscal year 1997, Datatronix' salespeople, managers, and others fraudulently inflated quarterly and annual revenues and earnings in violation of GAAP. The violations included the following:

1. Backdating license sale agreements
2. Entering into side agreements granting rights to refunds and other concessions to customers

3. Recognizing revenue on transactions with reseller customers that were not creditworthy
4. Recognizing amounts due under software maintenance agreements as software license revenues
5. Recognizing revenue on disputed claims against customers

Managers later explained that the frauds occurred when the performance numbers failed to meet the internal revenue and earnings objectives that in turn had been established to meet analysts' forecasts. As the quarterly cutoff dates approached, the sales department tried to close as many sales as possible to meet the quarterly objectives. If license agreements could not be signed before the end of the quarter, they were frequently signed later and backdated to the quarter in violation of both GAAP for revenue recognition and written internal policy. This practice was possible because of slack internal controls. Salespersons, the very people under pressure to produce good revenue figures, were responsible for overseeing the dating of signatures on agreements. In one known case, an agreement was accepted a month after the end of the quarter.

Written and oral side agreements were also common means of juggling revenues and earnings. The agreements had a wide variety of provisions, including the following:

1. Allowing resellers to return and to receive a refund or credit for unsold licenses
2. Committing the Company to use its own sales force to find customers for resellers
3. Offering to assign future end-user orders to resellers
4. Extending payment dates beyond twelve months
5. Committing the Company to purchase computer hardware or services from customers under terms that effectively refunded all or a substantial portion of the license fees paid by the customer
6. Diverting the Company's own future service revenues to customers as a means of refunding their license fees
7. Paying fictitious consulting or other fees to customers to be repaid to the Company as license fees

These side letters allowed the sales staff to "park" software licenses with resellers and bring them into revenue without actually having sold anything to an end user, indeed, without having even found an end user. The most notorious reseller involved in this scheme was known as the *bank* and the *virtual warehouse.* This reseller was, however, not very effective at moving Datatronix's products. Nevertheless, it entered into purchase agreements for $9.5 million in software licenses in fiscal 1995 but sold only $2.8 million in that year. In the first half of fiscal 1996, it entered into purchase agreements for an additional $5.9 million. During the *whole* of 1996, it sold only $6.2 million of the remaining $6.7 million in licenses purchased in 1995 and *none* of the $5.9 million in licenses purchased in the first two quarters of 1996.

Datatronix created these sales through a series of side letters inducing this reseller to enter into quarter-end purchase agreements. The Datatronix sales staff offered the bait of allowing the reseller to book a sale *they* were negotiating with an end user. The same arrangement with the same end user was offered to two other resellers. The result allowed Datatronix to book the same end-user sale three times through the three resellers.

Other side letters allowed resellers to cancel purchase agreements while Datatronix continued to recognize the original sales as revenue. One agreement allowed a reseller to cancel $6 million in licensing agreements in the third quarter of 1996. This figure represented 14 percent of pretax income for that quarter. Another side letter permitted a different reseller to cancel $6.4 million or 11 percent of the pretax income in the fourth quarter.

Additional GAAP violations occurred when service agreements were recognized as license sales and taken fully into revenue in a single quarter instead of being taken in ratably over the life of the contract. In the 1996 fourth quarter, three service agreement renewals totaling $11.2 million or 25 percent of pretax income for the period were treated as license sales and taken into revenue.

In the last quarter of 1995, Datatronix invoiced a customer for $5.4 million claiming the customer had used more copies of Datatronix's software than had been permitted under its license agreement. Finance staff thought the claim would be settled at a discount to the list price; the customer was told the $5.4 million could be applied against future purchases. The claim was settled in the first quarter of 1996 for $3.8 million but Datatronix improperly recognized the claim as fourth-quarter 1995 revenue and increased pretax income for the period by 13 percent. The remaining $1.8 million should have been written off in first-quarter 1996 but was instead improperly characterized as an unbilled maintenance fee receivable that was eventually written off over the last three quarters of fiscal 1996.

Revenue was recognized from end users with whom no contract had been signed and from whom no formal acceptance had been received. Policies for recognizing creditworthiness were disregarded and revenues were booked from under-capitalized and new customers. Both these actions are in clear violation of the GAAP that clearly states that "until persuasive evidence of the agreement exists and an assessment of the customer's creditworthiness has been made," no revenues can be recognized. Such improperly recognized revenues amounted to $3.3 million in the 1996 first quarter, $9.1 in the second, and $8.2 in the third.

At the end of the fourth quarter of fiscal 1996, Datatronix sold $9.2 million worth of software to a computer manufacturer for resale installed on its computers. Datatronix, however, failed to deliver the software code before the end of the fiscal year. Early in fiscal 1997, Datatronix delivered a so-called "beta" version that did not work on the purchaser's hardware. Usable software was not, in fact, delivered until more than half way through 1997. Revenue from the sale was improperly recognized, however, in the fourth quarter of 1996 and increased pretax income for the period by 13 percent.

In 1996, Datatronix decided to open so-called Megastores where it would team up with hardware providers to sell hardware-software solutions. So-called *partnerships* were formed with hardware providers whereby Datatronix would buy computers for the stores while the hardware providers would buy licensing agreements of equal or greater value than the hardware purchases. The hardware purchasers were also asked to buy licenses for the software installed in the demonstration computers in the Megastores. The hardware purchases and license sales were in cash and structured so the hardware purchase would give the providers cash flow at about the time the license agreement payments were due. All these transactions were premised on the expectation that Datatronix would absorb the costs of setting up new stores and that the Datatronix sales force would be involved in selling the solution as the hardware providers sales people were not familiar with the Datatronix software. Because of the high cost of opening and operating the Megastores, the costs of reselling licensing agreements were going to be high for Datatronix. To cover these costs, Datatronix offered its sales force higher commissions if sales were closed through the hardware providers rather than by Datatronix. Objectives were established for end-user sales to be applied against the hardware providers' outstanding commitments.

Datatronix recognized revenue when the hardware providers agreed to the purchase commitments even though Datatronix itself was paying the costs and expenses of setting up and operating the Megastores and its own sales force was going to do most of the reselling. This arrangement was in clear violation of the GAAP that if "other vendor obligations remaining after delivery are significant, revenue should not be recognized, because the earnings process is not substantially complete."

Datatronix committed these violations of GAAP and included this false information in its interim and annual financial statements. Information was also omitted or misrepresented in these statements and those filed with the SEC. As a result, the company's reports and filings were false and misleading.

At the end of March 1997, when the company announced a revenue shortfall, the stock price dropped 34.5 percent to $9 29/32 from $15 1/8 and reduced the Datatronix market capitalization to $1.5 billion from $2.3 billion. About two weeks after this collapse, CPAs began to hear about accounting irregularities in 1995 and 1996. Management realized that if the truth came out there would have to be a restatement and they resisted further investigation by indulging in additional fraudulent behavior for the purpose of limiting the scope of the audit. Over the next few months, nevertheless, more of the story began to emerge and by early September 1997, more than $100 million in various irregularities had been identified on the previously issued financial statements. On the basis of these revelations, amended 10-Ks and 10-Qs were filed with the SEC.

In the face of the SEC's intention to institute administrative proceedings against Datatronix, the company submitted an Offer of Settlement which the SEC accepted.

Conclusion and Analysis. The root of the problem seems to have been a lack of internal controls strong enough to permit the preparation of financial statements within GAAP. The effect of this lack of controls was magnified by an organizational structure that had important financial people responsible for revenue recognition reporting directly to sales personnel rather than to senior financial management.

Sales people under pressure to produce revenues to support analysts' forecasts were thus able to put pressure on their immediate financial superiors to recognize revenues not generated in accordance with GAAP.

10.5 FINANCIAL STATEMENT FRAUD CHECKLIST

The following checklist (table 10.4) addresses internal controls issues, taken from the discussion in this chapter, specific to suspected financial statement fraud. The checklist is an addition to the Risk Management checklist in chapter 1, "Managing the Risk of Fraud," Section 1.5, "Risk Management Checklist," and other checklists found in other sections of "The Fraud Handbook".

TABLE 10.4 FINANCIAL STATEMENT FRAUD CHECKLIST

Financial Statement Fraud Checklist	Yes	No	NA	Ref
1. Motives				
A yes *answer to any of the questions in this section indicates a greater likelihood of potential financial statement fraud.*				
a. Is there a perception among management of the company or individual operating units that there is extraordinary pressure (over and above the pressures typically associated with this industry) to achieve a higher level of reported earnings?	☐	☐	☐	___
b. Do management compensation agreements tie compensation or bonuses to higher levels of reported earnings?	☐	☐	☐	___
c. Is there extraordinary pressure from outside shareholders or other outsiders to improve the value of company stock?	☐	☐	☐	___
d. With regard to shares held by management or major shareholders, could the existence of any of the following provide an incentive to maintain or increase reported earnings, especially in the near term?	☐	☐	☐	___
• Vesting provisions in employee stock ownership plans that postpone ownership	☐	☐	☐	___
• Stock option exercise restrictions that prevent managers from acquiring shares until specified dates or the occurrence of specific events	☐	☐	☐	___
• Rule 144A restrictions that limit the number of shares that can be sold on U. S. securities exchanges on a given trading day	☐	☐	☐	___
• Income tax provisions that afford more favorable treatment to capital gains in shares held for a sufficient period of time to qualify as long-term capital gains (the restriction being that the government would receive more of the sale proceeds if the share sales were classified as short-term capital gains)	☐	☐	☐	___
• Corporate control requirements that necessitate holding significant blocks of stock past some event such as an annual shareholders meeting before they can be sold	☐	☐	☐	___
e. Is the company in danger of losing its listing on a major stock exchange, or is it attempting to obtain a new listing?	☐	☐	☐	___
f. Is there extraordinary pressure, whether explicit or implicit, to continue to report a rising trend in earnings and/or revenues?	☐	☐	☐	___

(continued)

TABLE 10.4 *(continued)*

Financial Statement Checklist	**Yes**	**No**	**NA**	**Ref**
g. Is the company operating close to or in violation of the limits of financial covenants, such as minimum shareholders' equity, maximum debt-to-equity ratios, or minimum current ratios, contained in bank credit facility agreements or other debt instruments?	☐	☐	☐	___
h. For firms doing business in regulated industries, is the company operating close to or in violation of the financial restrictions set by regulators or by statute?	☐	☐	☐	___
2. Quantitative Characteristics				
A yes *answer to any of the questions in this section indicates a greater likelihood of potential financial statement fraud.*				
a. When calculating the following indexes for the previous and the current year, do any of the indexes show a year-over-year increase greater than 10 percent (meaning, an index greater than 1.1)?	☐	☐	☐	___
• Days' Sales in Receivables Index	☐	☐	☐	___
• Gross Margin Index	☐	☐	☐	___
• Asset Quality Margin Index	☐	☐	☐	___
• Sales Growth Index	☐	☐	☐	___
b. When calculating the following indexes for the previous and the current year, do any of the indexes show a year-over-year increase greater than 10 percent more than increases for similar indexes of peer (same industry) companies?	☐	☐	☐	___
• Days' Sales in Receivables Index	☐	☐	☐	___
• Gross Margin Index	☐	☐	☐	___
• Asset Quality Index	☐	☐	☐	___
• Sale's Growth Index	☐	☐	☐	___
c. Is the change in working capital over the past year (excluding cash changes) relative to total assets at the end of the period more than 20 percent greater than similar calculations for peer companies?	☐	☐	☐	___
3. Qualitative Predictors: The Audit Committee				
A yes *answer to any of the questions in this section indicates a need to take action to improve the integrity and effectiveness of the Audit Committee.*				
a. Has the board of directors failed to designate an audit committee or failed to approve a charter for an audit committee?	☐	☐	☐	___

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
b. If there is an audit committee, do any of the following conditions exist with regard to members of that committee?	☐	☐	☐	___
• A director being employed by the corporation or any of its affiliates for the current year or any of the past five years	☐	☐	☐	___
• A director accepting any compensation from the corporation or any of its affiliates other than compensation for board service or benefits under a tax-qualified retirement plan	☐	☐	☐	___
• A director being a member of the immediate family of an individual who is or has been in any of the past five years employed by the corporation or any of its affiliates as an executive officer	☐	☐	☐	___
• A director being a partner in or a controlling shareholder, or to which the corporation made, or from which the corporation received, payments that are or have been significant to the corporation or business organization in any of the past five years	☐	☐	☐	___
• A director being employed as an executive of another company while any of the corporation's executives serves on that company's compensation committee	☐	☐	☐	___
c. Are there less than three audit committee members with at least some financial accounting experience?	☐	☐	☐	___
d. Is it not clear or not the case that the audit committee–				
• Should be responsible for selecting the outside auditors?	☐	☐	☐	___
• Has a formal written statement from the outside auditors describing all relationships between the auditors and the company?	☐	☐	☐	___
• Regularly discusses with the outside auditors all aspects of the propriety or lack thereof of the company's accounting practices?	☐	☐	☐	___
• Receives all reports of internal control deficiencies in a timely manner from both internal and outside auditors?	☐	☐	☐	___
4. Other Qualitative Predictors				
A yes *answer to any of the questions in this section indicates a greater likelihood of potential financial statement fraud.*				
a. Has the company had a history of internal control problems, whether those problems resulted in the detection of financial statement or any other type of fraud?	☐	☐	☐	___

(continued)

Table 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
b. Does the company chief executive officer engage in micro-management or other practices that could unduly influence accounting decision-makers with regard to financial statement reporting?	☐	☐	☐	___
c. Are outside auditors unaware of any interim or quarterly financial statements or financial statements prepared for selected outside parties such as banks or investors?	☐	☐	☐	___
d. In establishing and reviewing internal controls, has management failed to establish adequately the key metrics or guidelines to determine the extent and frequency of internal auditor review?	☐	☐	☐	___
e. Is there a lack of evidence that management has properly communicated the internal control guidelines and procedures to appropriate personnel?	☐	☐	☐	___
f. Does it appear that management does not assess the quality of its internal controls over time?	☐	☐	☐	___
g. Have any audit tests detected significant risks not previously known to management?	☐	☐	☐	___
h. Is there a history of using a quantitative standard for materiality, such as a percentage of earnings or assets, to fail to correct known accounting errors or irregularities?	☐	☐	☐	___
5. Special Areas				
A yes *answer to any of the questions in this section should generate further inquiry to determine if specific internal controls need to be improved.*				
Failure to Record Loss Contingencies				
a. Given the nature of the company's business, is it likely that any of the following issues could be relevant?	☐	☐	☐	___
• Collectibility of receivables	☐	☐	☐	___
• Obligations related to product warranties and product defects	☐	☐	☐	___
• Risk of loss or damage of enterprise property	☐	☐	☐	___
• Threat of expropriation of assets	☐	☐	☐	___
• Pending or threatened litigation	☐	☐	☐	___
• Actual or possible claims and assessments	☐	☐	☐	___
• Guarantees of indebtedness of others	☐	☐	☐	___
• Agreements to repurchase receivables (or repurchase related property) that have been sold	☐	☐	☐	___

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
b. With regard to possible contingencies, do any of the following exist?	☐	☐	☐	___
• The incidence of claims prior to the date of financial statements	☐	☐	☐	___
• Correspondence with (and bills from) outside legal counsel	☐	☐	☐	___
• Internal correspondence within production and research staffs as to the need to address a critical problem with a product already on the market	☐	☐	☐	___
• Internal correspondence among department heads of production, R&D, general counsel, and senior management about postproduction problems and product claims	☐	☐	☐	___
• External correspondence between the manufacturer and its customers about a given product concerning special price concessions or special return privileges	☐	☐	☐	___
• The incidence of special or over budget freight charges to accommodate returns and/or the shipment of replacement product	☐	☐	☐	___
• Shifting of production schedules to manufacture replacement product	☐	☐	☐	___
• Halting manufacture of the product in question	☐	☐	☐	___
• Shifting of R&D staff away from planned research projects to applications engineering relating to redesign of existing products	☐	☐	☐	___
• Payments in sometimes seemingly immaterial amounts to customers on a regular basis over a period of weeks or months that indicate some arrangement to compensate for product defects	☐	☐	☐	___
c. If there is a suspected contingency, does correspondence between departments or within departments indicate a problem?	☐	☐	☐	___
d. If a contingency is likely to exist, has management used an inadequate or inappropriate standard for quantifying the potential claim?	☐	☐	☐	___
Failure to Record Asset Writeoffs				
a. Has the company's industry experienced rapid changes in engineering or materials applications that may lead to asset writeoffs?	☐	☐	☐	___

(continued)

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
b. Is the industry in which the company operates very cost competitive?	☐	☐	☐	___
c. Has the company experienced any of the following?	☐	☐	☐	___
• Significant changes in customer demand	☐	☐	☐	___
• Significant loss of business to a competitor	☐	☐	☐	___
• A need to obtain or retain a customer relationship by bidding below cost	☐	☐	☐	___
d. When reviewing fixed asset schedules with production or divisional personnel, have any of the following occurred?				
• A significant decrease in the market value of an asset	☐	☐	☐	___
• A significant change in the extent or manner in which an asset is used or a significant physical change in an asset	☐	☐	☐	___
• A significant adverse change in legal factors or in the business climate that could affect the value of an asset or an adverse action or assessment by a regulator	☐	☐	☐	___
• An accumulation of costs significantly in excess of the amount originally expected to acquire or construct an asset	☐	☐	☐	___
• A current period operating or cash-flow loss combined with a history of operating or cash-flow losses or a projection or forecast that demonstrates continuing losses associated with an asset used for the purpose of producing revenue	☐	☐	☐	___
e. Is there evidence of significant changes in production or product demand?	☐	☐	☐	___
f. From the review of moving expenses and discussion with production personnel, does it appear that any equipment has been moved off the shop floor into storage?	☐	☐	☐	___
g. the company not maintain profitability analyses by product line or by customer?	☐	☐	☐	___
h. Upon reviewing profitability analyses, does it appear that certain products have not been historically profitable?	☐	☐	☐	___
i. For historically unprofitable product lines, to justify not writing down assets for impairment, has management used any of the following?	☐	☐	☐	___
• Overly optimistic forecasts of future profitability	☐	☐	☐	___
• Out-of-date forecasts	☐	☐	☐	___
• Forecasts not prepared or reviewed by personnel with line responsibility for production	☐	☐	☐	___

TABLE 10.4 *(continued)*

Financial Statement Checklist	**Yes**	**No**	**NA**	**Ref**
j. If written narratives accompany the forecasts, do they discuss downside possibilities that management has not adequately taken into account?	☐	☐	☐	___
k. Are there any facts now known that would invalidate assumptions contained in the forecast?	☐	☐	☐	___
l. For investments in non-publicly traded securities, have any of the following occurred?	☐	☐	☐	___
• Does the company have financial data adequate to determine historical profitability of the investee?	☐	☐	☐	___
• If the investee has not been historically profitable, has management failed to write down the investment based upon an overly optimistic forecast?	☐	☐	☐	___
• If the investee has not been historically profitable, has management failed to write down the investment based upon a forecast prepared by management with business or family ties to the investor company?	☐	☐	☐	___
Acquisition and Cookie Jar Reserves				
a. Were reserves established without a clear purpose or justification?	☐	☐	☐	___
b. If reserves were established by a current period charge to income, were earnings prior to the charge in excess of management or outside expectations?	☐	☐	☐	___
c. Were reserves established at or near the close of a reporting period?	☐	☐	☐	___
d. Were reserves established without adequate review by senior management?	☐	☐	☐	___
e. Upon review of charges to a given reserve, are there charges for expenses that are not appropriate to the stated purpose of the reserve?	☐	☐	☐	___
f. Was the timing of the takedown of reserves coincident with achieving certain financial targets set by management or outsiders?	☐	☐	☐	___
g. Was the amount of the takedown of reserves for a given period necessary to achieve certain financial targets set by management or outsiders?	☐	☐	☐	___
h. Has any of the following occurred with regard to acquisition reserves?	☐	☐	☐	___

(continued)

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
• Were reserves established after twelve months from the date of the acquisition?	☐	☐	☐	___
• Were reserves set up for items not related to the acquisition?	☐	☐	☐	___
• Does the quantity of costs allocated to the reserve in a given period cause earnings to reach certain financial targets set by management or outsiders?	☐	☐	☐	___
Cost Shifting				
a. Has management made a recent change in policy with regard to capitalizing previously expensed costs?	☐	☐	☐	___
b. Has a change in policy with regard to capitalizing previously expensed costs not been disclosed in company financial statements?	☐	☐	☐	___
c. Has management proposed to capitalize a new category of expenditure that customarily is expensed on peer-group firm financial statements?	☐	☐	☐	___
d. Does the timing of changes in policy with regard to capitalizing expenses coincide with any of the following?	☐	☐	☐	___
• Implementation of a management bonus plan or calculation of bonuses under that plan	☐	☐	☐	___
• Commencement of the sale of stock or the search for an equity partner	☐	☐	☐	___
• Implementation of a new credit facility or recent problems in maintaining financial covenants under an existing facility	☐	☐	☐	___
e. But for the capitalization of certain expenses, would any of the following occur?	☐	☐	☐	___
• Management would not receive certain bonuses or other benefits under a management compensation plan.	☐	☐	☐	___
• In the opinion of securities analysts, appraisers, or underwriters, the company's share price would be significantly lower.	☐	☐	☐	___
• The company would be in violation of loan or debt covenants.	☐	☐	☐	___
f. Does the capitalization of expenses cause the firm's Asset Quality Index to increase significantly in excess of increases (if any) for its industry peers?	☐	☐	☐	___

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
g. If company management provides segment or subsidiary financial data, especially if management or outsiders tend to point to performance of that segment or subsidiary in their discussions of company performance, has either of the following occurred?	☐	☐	☐	___
• Have expenses been incurred by the parent that relates to the segment or subsidiary?	☐	☐	☐	___
• Have other segments or subsidiaries incurred expenses that should be allocated to the segment or subsidiary in question?	☐	☐	☐	___
h. Has senior management failed to establish proper procedures for allocating or apportioning costs among affiliates or, if there is a policy, is there evidence that adherence is lax or that there have been documented lapses?	☐	☐	☐	___
i. Is there correspondence among heads of affiliates concerning disputes over expense allocations or apportionment that has not come to the attention of the audit committee?	☐	☐	☐	___
j. Were reserves established at the parent company for expenses anticipated for subsidiaries?	☐	☐	☐	___
k. Are there debit entries in subsidiary expense or liability accounts that could reflect cost transfers to the parent or another subsidiary?	☐	☐	☐	___
l. Are there debit entries in subsidiary expense or liability accounts that could reflect cost transfers to reserves established at the parent level or in another subsidiary?	☐	☐	☐	___
m. Is there any correspondence between accounting personnel at the parent and subsidiary levels that describe special procedures for certain costs that are incurred by the subsidiary but not charged to earnings of that subsidiary?	☐	☐	☐	___
Recording Fictitious Revenues				
a. If the company requires signed agreements from customers before revenue is recognized, have sales personnel indicated or stated any of the following?	☐	☐	☐	___
• Their managers have approved as income sales contracts that were not signed as of the period end.	☐	☐	☐	___
• Unsigned contracts were recorded as revenue under the premise that key buyer personnel had given verbal approvals.	☐	☐	☐	___
• Unsigned contracts were recorded as revenue under the premise that key buyer personnel had signed the contract but the contract was held up for other reasons.	☐	☐	☐	___

(continued)

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
b. Have there been prior internal control failures with sales cutoff?	☐	☐	☐	___
c. If fabricated contracts are suspected, have the sales cutoff tests performed by internal or outside auditors failed to look for the fabrication and substitution of contracts?	☐	☐	☐	___
d. Have sales cutoff tests failed to examine the history of sales returns and reversals over time?	☐	☐	☐	___
e. With regard to the requirement for timely delivery, has any of the following occurred?				
• Are there lapses in documentation of delivery?	☐	☐	☐	___
• Have customers complained about receiving deliveries too early?	☐	☐	☐	___
• Have returns from a certain customer or reseller been abnormally high?	☐	☐	☐	___
f. Is there evidence that certain customers or resellers are receiving unusually generous sales terms for returns or refunds?	☐	☐	☐	___
g. Is there evidence that certain customers or resellers are receiving unusually low prices or above-average discounts?	☐	☐	☐	___
h. Is the price for component products sold by the company dependent, at least in part, upon the price of the final product sold by another company?	☐	☐	☐	___
i. Have royalties been accrued to income prior to receipt of confirmation from the payor that royalties are owed?	☐	☐	☐	___
j. Do department heads have the authority to both approve sales and the recognition of related revenue in the financial statements?	☐	☐	☐	___
k. Is there a lack of review of sales revenue recognition at the senior management level?	☐	☐	☐	___
l. Is there a history of revenue being recognized improperly?	☐	☐	☐	___
m. Have department heads approved significant refunds or returns that are out of the ordinary or appear to violate company policies?	☐	☐	☐	___
n. Have refunds or returns been historically high for a certain department?	☐	☐	☐	___
o. Have the reasons for refunds and returns not been documented or, if documented, have the reasons given been insufficient?	☐	☐	☐	___

TABLE 10.4 *(continued)*

Financial Statement Checklist	Yes	No	NA	Ref
p. Has senior management failed to review or been lax in reviewing significant sales refunds and returns?	☐	☐	☐	___
q. If side letters are suspected, has either of the following occurred?	☐	☐	☐	___
• Engineers, technicians, or others involved with the installation of the products indicated that certain customers made additional demands before agreeing to buy.	☐	☐	☐	___
• There are notes or letters in sales files indicating that customer demands had been made to allow for returns or refunds.	☐	☐	☐	___
r. Are sales approved before obtaining credit checks for new customers or for existing customers that are experiencing financial difficulties?	☐	☐	☐	___
s. Is there an unusual concentration of orders from small or distressed customers occurring near the end of a reporting period or sales contest?	☐	☐	☐	___

Appendix:

SEC Staff Accounting Bulletin (SAB) No. 99

SEC Staff Accounting Bulletin:
No. 99–Materiality

SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 211

[Release No. SAB 99]

Staff Accounting Bulletin No. 99

AGENCY: Securities and Exchange Commission

ACTION: Publication of Staff Accounting Bulletin

SUMMARY: This staff accounting bulletin expresses the views of the staff that exclusive reliance on certain quantitative benchmarks to assess materiality in preparing financial statements and performing audits of those financial statements is inappropriate; misstatements are not immaterial simply because they fall beneath a numerical threshold.

DATE: August 12, 1999

FOR FURTHER INFORMATION CONTACT: W. Scott Bayless, Associate Chief Accountant, or Robert E. Burns, Chief Counsel, Office of the Chief Accountant (202-942-4400), or David R. Fredrickson, Office of General Counsel (202-942-0900), Securities and Exchange Commission, 450 Fifth Street, N.W., Washington, D.C. 20549-1103; electronic addresses: BaylessWS@sec.gov; BurnsR@sec.gov; FredricksonD@sec.gov.

SUPPLEMENTARY INFORMATION: The statements in the staff accounting bulletins are not rules or interpretations of the Commission, nor are they published as bearing the Commission's official approval. They represent interpretations and practices followed by the Division of Corporation Finance and the Office of the Chief Accountant in administering the disclosure requirements of the Federal securities laws.

Jonathan G. Katz

Secretary

Date: August 12, 1999

Part 211–(AMEND) Accordingly, Part 211 of Title 17 of the Code of Federal Regulations is amended by adding Staff Accounting Bulletin No. 99 to the table found in Subpart B.

STAFF ACCOUNTING BULLETIN NO. 99

The staff hereby adds Section M to Topic 1 of the Staff Accounting Bulletin Series. Section M, entitled "Materiality," provides guidance in applying materiality thresholds to the preparation of financial statements filed with the Commission and the performance of audits of those financial statements.

STAFF ACCOUNTING BULLETINS

TOPIC 1: FINANCIAL STATEMENTS

* * * * *

M. Materiality

1. Assessing Materiality

Facts: During the course of preparing or auditing year-end financial statements, financial management or the registrant's independent auditor becomes aware of misstatements in a registrant's financial statements. When combined, the misstatements result in a 4% overstatement of net income and a \$.02 (4%) overstatement of earnings per share. Because no item in the registrant's consolidated financial statements is misstated by more than 5%, management and the independent auditor conclude that the deviation from generally accepted accounting principles ("GAAP") is immaterial and that the accounting is permissible.[1]

Question: Each Statement of Financial Accounting Standards adopted by the Financial Accounting Standards Board ("FASB") states, "The provisions of this Statement need not be applied to immaterial items." In the staff's view, may a registrant or the auditor of its financial statements assume the immateriality of items that fall below a percentage threshold set by management or the auditor to determine whether amounts and items are material to the financial statements?

Interpretive Response: No. The staff is aware that certain registrants, over time, have developed quantitative thresholds as "rules of thumb" to assist in the preparation of their financial statements, and that auditors also have used these thresholds in their evaluation of whether items might be considered material to users of a registrant's financial statements. One rule of thumb in particular suggests that the misstatement or omission[2] of an item that falls under a 5% threshold is not material in the absence of particularly egregious circumstances, such as self-dealing or misappropriation by senior management. The staff reminds registrants and the auditors of their financial statements that exclusive reliance on this or any percentage or numerical threshold has no basis in the accounting literature or the law.

The use of a percentage as a numerical threshold, such as 5%, may provide the basis for a preliminary assumption that–without considering all relevant circumstances–a deviation of less than the specified percentage with respect to a particular item on the registrant's financial statements is unlikely to be material. The staff has no objection to such a "rule of thumb" as an initial step in assessing materiality. But quantifying, in percentage terms, the magnitude of a misstatement is only the beginning of an analysis of materiality; it cannot appropriately be used as a substitute for a full analysis of all relevant considerations. Materiality concerns the significance of an item to users of a registrant's financial statements. A matter is "material" if there is a substantial likelihood that a reasonable person would consider it important. In its Statement of Financial Accounting Concepts No. 2, the FASB stated the essence of the concept of materiality as follows:

> The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.[3]

This formulation in the accounting literature is in substance identical to the formulation used by the courts in interpreting the federal securities laws. The Supreme Court has held that a fact is material if there is–

> a substantial likelihood that the . . . fact would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available. [4]

Under the governing principles, an assessment of materiality requires that one views the facts in the context of the "surrounding circumstances," as the accounting literature puts it, or the "total mix" of information, in the words of the Supreme Court. In the context of a misstatement of a financial statement item, while the "total mix" includes the size in numerical or percentage terms of the misstatement, it also includes the factual context in which the user of financial statements would view the financial statement item. The shorthand in the accounting and auditing literature for this analysis is that financial management and the auditor must consider both "quantitative" and "qualitative" factors in assessing an item's materiality.[5] Court decisions, Commission rules and enforcement actions, and accounting and auditing literature[6] have all considered "qualitative" factors in various contexts.

The FASB has long emphasized that materiality cannot be reduced to a numerical formula. In its Concepts Statement No. 2, the FASB noted that some had urged it to promulgate quantitative materiality guides for use in a variety of situations. The FASB rejected such an approach as representing only a "minority view," stating–

> The predominant view is that materiality judgments can properly be made only by those who have all the facts. The Board's present position is that no general standards of materiality could be formulated to take into account all the considerations that enter into an experienced human judgment. [7]

The FASB noted that, in certain limited circumstances, the Commission and other authoritative bodies had issued quantitative materiality guidance, citing as examples guidelines ranging from one to ten percent with respect to a variety of disclosures.[8] And it took account of contradictory studies, one showing a lack of uniformity among auditors on materiality judgments, and another suggesting widespread use of a "rule of thumb" of five to ten percent of net income.[9] The FASB also considered whether an evaluation of materiality could be based solely on anticipating the market's reaction to accounting information.[10]

The FASB rejected a formulaic approach to discharging "the onerous duty of making materiality decisions"[11] in favor of an approach that takes into account all the relevant considerations. In so doing, it made clear that–

> [M]agnitude by itself, without regard to the nature of the item and the circumstances in which the judgment has to be made, will not generally be a sufficient basis for a materiality judgment.[12]

Evaluation of materiality requires a registrant and its auditor to consider *all* the relevant circumstances, and the staff believes that there are numerous circumstances in which misstatements below 5% could well be material. Qualitative factors may cause misstatements of quantitatively small amounts to be material; as stated in the auditing literature:

> As a result of the interaction of quantitative and qualitative considerations in materiality judgments, misstatements of relatively small amounts that come to the auditor's attention could have a material effect on the financial statements.[13]

Among the considerations that may well render material a quantitatively small misstatement of a financial statement item are–

> whether the misstatement arises from an item capable of precise measurement or whether it arises from an estimate and, if so, the degree of imprecision inherent in the estimate[14]
>
> whether the misstatement masks a change in earnings or other trends
>
> whether the misstatement hides a failure to meet analysts' consensus expectations for the enterprise
>
> whether the misstatement changes a loss into income or vice versa
>
> whether the misstatement concerns a segment or other portion of the registrant's business that has been identified as playing a significant role in the registrant's operations or profitability
>
> whether the misstatement affects the registrant's compliance with regulatory requirements
>
> whether the misstatement affects the registrant's compliance with loan covenants or other contractual requirements
>
> whether the misstatement has the effect of increasing management's compensation–for example, by satisfying requirements for the award of bonuses or other forms of incentive compensation
>
> whether the misstatement involves concealment of an unlawful transaction.

This is not an exhaustive list of the circumstances that may affect the materiality of a quantitatively small misstatement.[15] Among other factors, the demonstrated volatility of the price of a registrant's securities in response to certain types of disclosures may provide guidance as to whether investors regard quantitatively small misstatements as material. Consideration of potential market reaction to disclosure of a misstatement is by itself "too blunt an instrument to be depended on" in considering whether a fact is material.[16] When, however, management or the independent auditor expects (based, for example, on a pattern of market performance) that a known misstatement may result in a significant positive or negative market reaction, that expected reaction should be taken into account when considering whether a misstatement is material.[17]

For the reasons noted above, the staff believes that a registrant and the auditors of its financial statements should not assume that even small intentional misstatements in financial statements, for example those pursuant to actions to "manage" earnings, are immaterial.[18] While the intent of management does not render a misstatement material, it may provide significant evidence of materiality. The evidence may be particularly compelling where management has intentionally misstated items in the financial statements to "manage" reported earnings. In that instance, it presumably has done so believing that the resulting amounts and trends would be significant to users of the registrant's financial statements.[19] The staff believes that investors generally would regard as significant a management practice to over- or under-state earnings up to an amount just short of a percentage threshold in order to "manage" earnings. Investors presumably also would regard as significant an accounting practice that, in essence, rendered all earnings figures subject to a management-directed margin of misstatement.

The materiality of a misstatement may turn on where it appears in the financial statements. For example, a misstatement may involve a segment of the registrant's operations. In that instance, in assessing materiality of a misstatement to the financial statements taken as a whole, registrants and their auditors should consider not only the size of the misstatement but also the significance of the segment information to the financial statements taken as a whole.[20] "A misstatement of the revenue and operating profit of a relatively small segment that is represented by management to be important to the future profitability of the entity"[21] is more likely to be material to investors than a misstatement in a segment that management has not identified as especially important. In assessing the materiality of misstatements in segment information–as with materiality generally–

> situations may arise in practice where the auditor will conclude that a matter relating to segment information is qualitatively material even though, in his or her judgment, it is quantitatively immaterial to the financial statements taken as a whole.[22]

Aggregating and Netting Misstatements

In determining whether multiple misstatements cause the financial statements to be materially misstated, registrants and the auditors of their financial statements should consider each misstatement separately and the aggregate effect of all misstatements.[23] A registrant and its auditor should evaluate misstatements in light of quantitative and qualitative factors and "consider whether, in relation to individual line item amounts, subtotals, or totals in the financial statements, they materially misstate the financial statements taken as a whole."[24] This requires consideration of–

> the significance of an item to a particular entity (for example, inventories to a manufacturing company), the pervasiveness of the misstatement (such as whether it affects the presentation of numerous financial statement items), and the effect of the misstatement on the financial statements taken as a whole . . . .[25]

Registrants and their auditors first should consider whether each misstatement is material, irrespective of its effect when combined with other misstatements. The literature notes that the analysis should consider whether the misstatement of "individual amounts" causes a material misstatement of the financial statements taken as a whole. As with materiality generally, this analysis requires consideration of both quantitative and qualitative factors.

If the misstatement of an individual amount causes the financial statements as a whole to be materially misstated, that effect cannot be eliminated by other misstatements whose effect may be to diminish the impact of the misstatement on other financial statement items. To take an obvious example, if a registrant's revenues are a material financial statement item and if they are materially overstated, the financial statements taken as a whole will be materially misleading even if the effect on earnings is completely offset by an equivalent overstatement of expenses.

Even though a misstatement of an individual amount may not cause the financial statements taken as a whole to be materially misstated, it may nonetheless, when aggregated with other misstatements, render the financial statements taken as a whole to be materially misleading. Registrants and the auditors of their financial statements accordingly should consider the effect of the misstatement on subtotals or totals. The auditor should aggregate all misstatements that affect each subtotal or total and consider whether the misstatements in the aggregate affect the subtotal or total in a way that causes the registrant's financial statements taken as a whole to be materially misleading.[26]

The staff believes that, in considering the aggregate effect of multiple misstatements on a subtotal or total, registrants and the auditors of their financial statements should exercise particular care when considering whether to offset (or the appropriateness of offsetting) a misstatement of an estimated amount with a misstatement of an item capable of precise measurement. As noted above, assessments of materiality should never be purely mechanical; given the imprecision inherent in estimates, there is by definition a corresponding imprecision in the aggregation of misstatements involving estimates with those that do not involve an estimate.

Registrants and auditors also should consider the effect of misstatements from prior periods on the current financial statements. For example, the auditing literature states,

> Matters underlying adjustments proposed by the auditor but not recorded by the entity could potentially cause future financial statements to be materially misstated, even though the auditor has concluded that the adjustments are not material to the current financial statements.[27]

This may be particularly the case where immaterial misstatements recur in several years and the cumulative effect becomes material in the current year.

2. Immaterial Misstatements That are Intentional

Facts: A registrant's management intentionally has made adjustments to various financial statement items in a manner inconsistent with GAAP. In each accounting period in which such actions were taken, none of the individual adjustments is by itself material, nor is the aggregate effect on the financial statements taken as a whole material for the period. The registrant's earnings "management" has been effected at the direction or acquiescence of management in the belief that any deviations from GAAP have been immaterial and that accordingly the accounting is permissible.

Question: In the staff's view, may a registrant make intentional immaterial misstatements in its financial statements?

Interpretive Response: No. In certain circumstances, intentional immaterial misstatements are unlawful.

Considerations of the Books and Records Provisions Under the Exchange Act

Even if misstatements are immaterial,[28] registrants must comply with Sections 13(b)(2)-(7) of the Securities Exchange Act of 1934 (the "Exchange Act").[29] Under these provisions, each registrant with securities registered pursuant to Section 12 of the Exchange Act,[30] or required to file reports pursuant to Section 15(d),[31] must make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets of the registrant and must maintain internal accounting controls that are sufficient to provide reasonable assurances that, among other things, transactions are recorded as necessary to permit the preparation of financial statements in conformity with GAAP.[32] In this context, determinations of what constitutes "reasonable assurance" and "reasonable detail" are based not on a "materiality" analysis but on the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs.[33] Accordingly, failure to record accurately immaterial items, in some instances, may result in violations of the securities laws.

The staff recognizes that there is limited authoritative guidance[34] regarding the "reasonableness" standard in Section 13(b)(2) of the Exchange Act. A principal statement of the Commission's policy in this area is set forth in an address given in 1981 by then Chairman Harold M. Williams.[35] In his address, Chairman Williams noted that, like materiality, "reasonableness" is not an "absolute standard of exactitude for corporate records."[36] Unlike materiality, however, "reasonableness" is not solely a measure of the significance of a financial statement item to investors. "Reasonableness," in this context, reflects a judgment as to whether an issuer's failure to correct a known misstatement implicates the purposes underlying the accounting provisions of Sections 13(b)(2)-(7) of the Exchange Act.[37]

In assessing whether a misstatement results in a violation of a registrant's obligation to keep books and records that are accurate "in reasonable detail," registrants and their auditors should consider, in addition to the factors discussed above concerning an evaluation of a misstatement's potential materiality, the factors set forth below.

The significance of the misstatement. Though the staff does not believe that registrants need to make finely calibrated determinations of significance with respect to immaterial items, plainly it is "reasonable" to treat misstatements whose effects are clearly inconsequential differently than more significant ones.

How the misstatement arose. It is unlikely that it is ever "reasonable" for registrants to record misstatements or not to correct known misstatements–even immaterial ones–as part of an ongoing effort directed by or known to senior management for the purposes of "managing" earnings. On the other hand, insignificant misstatements that arise from the operation of systems or recurring processes in the normal course of business generally will not cause a registrant's books to be inaccurate "in reasonable detail."[38]

The cost of correcting the misstatement. The books and records provisions of the Exchange Act do not require registrants to make major expenditures to correct small misstatements.[39] Conversely, where there is little cost or delay involved in correcting a misstatement, failing to do so is unlikely to be "reasonable."

> **The clarity of authoritative accounting guidance with respect to the misstatement.** Where reasonable minds may differ about the appropriate accounting treatment of a financial statement item, a failure to correct it may not render the registrant's financial statements inaccurate "in reasonable detail." Where, however, there is little ground for reasonable disagreement, the case for leaving a misstatement uncorrected is correspondingly weaker.

There may be other indicators of "reasonableness" that registrants and their auditors may ordinarily consider. Because the judgment is not mechanical, the staff will be inclined to continue to defer to judgments that "allow a business, acting in good faith, to comply with the Act's accounting provisions in an innovative and cost-effective way."[40]

The Auditor's Response to Intentional Misstatements

Section 10A(b) of the Exchange Act requires auditors to take certain actions upon discovery of an "illegal act."[41] The statute specifies that these obligations are triggered "whether or not [the illegal acts are] perceived to have a material effect on the financial statements of the issuer . . . ." Among other things, Section 10A(b)(1) requires the auditor to inform the appropriate level of management of an illegal act (unless clearly inconsequential) and assure that the registrant's audit committee is "adequately informed" with respect to the illegal act.

As noted, an intentional misstatement of immaterial items in a registrant's financial statements may violate Section 13(b)(2) of the Exchange Act and thus be an illegal act. When such a violation occurs, an auditor must take steps to see that the registrant's audit committee is "adequately informed" about the illegal act. Because Section 10A(b)(1) is triggered regardless of whether an illegal act has a material effect on the registrant's financial statements, where the illegal act consists of a misstatement in the registrant's financial statements, the auditor will be required to report that illegal act to the audit committee irrespective of any "netting" of the misstatements with other financial statement items.

The requirements of Section 10A echo the auditing literature. See, for example, Statement on Auditing Standards No. ("SAS") 54, "Illegal Acts by Clients," and SAS 82, "Consideration of Fraud in a Financial Statement Audit." Pursuant to paragraph 38 of SAS 82, if the auditor determines there is evidence that fraud may exist, the auditor must discuss the matter with the appropriate level of management. The auditor must report directly to the audit committee fraud involving senior management and fraud that causes a material misstatement of the financial statements. Paragraph 4 of SAS 82 states that "misstatements arising from fraudulent financial reporting are intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users."[42] SAS 82 further states that fraudulent financial reporting may involve falsification or alteration of accounting records; misrepresenting or omitting events, transactions or other information in the financial statements; and the intentional misapplication of accounting principles relating to amounts, classifications, the manner of presentation, or disclosures in the financial statements.[43] The clear implication of SAS 82 is that immaterial misstatements may be fraudulent financial reporting. [44]

Auditors that learn of intentional misstatements may also be required to (1) re-evaluate the degree of audit risk involved in the audit engagement, (2) determine whether to revise the nature, timing, and extent of audit procedures accordingly, and (3) consider whether to resign.[45]

Intentional misstatements also may signal the existence of reportable conditions or material weaknesses in the registrant's system of internal accounting control designed to detect and deter improper accounting and financial reporting.[46] As stated by the National Commission on Fraudulent Financial Reporting, also known as the Treadway Commission, in its 1987 report,

> The tone set by top management–the corporate environment or culture within which financial reporting occurs–is the most important factor contributing to the integrity of the financial reporting process. Notwithstanding an impressive set of written rules and procedures, if the tone set by management is lax, fraudulent financial reporting is more likely to occur.[47]

An auditor is required to report to a registrant's audit committee any reportable conditions or material weaknesses in a registrant's system of internal accounting control that the auditor discovers in the course of the examination of the registrant's financial statements.[48]

GAAP Precedence Over Industry Practice

Some have argued to the staff that registrants should be permitted to follow an industry accounting practice even though that practice is inconsistent with authoritative accounting literature. This situation might occur if a practice is developed when there are few transactions and the accounting results are clearly inconsequential, and that practice never changes despite a subsequent growth in the number or materiality of such transactions. The staff disagrees with this argument. Authoritative literature takes precedence over industry practice that is contrary to GAAP.[49]

General Comments

This SAB is not intended to change current law or guidance in the accounting or auditing literature.[50] This SAB and the authoritative accounting literature cannot specifically address all of the novel and complex business transactions and events that may occur. Accordingly, registrants may account for, and make disclosures about, these transactions and events based on analogies to similar situations or other factors. The staff may not, however, always be persuaded that a registrant's determination is the most appropriate under the circumstances. When disagreements occur after a transaction or an event has been reported, the consequences may be severe for registrants, auditors, and, most importantly, the users of financial statements who have a right to expect consistent accounting and reporting for, and disclosure of, similar transactions and events. The staff, therefore, encourages registrants and auditors to discuss on a timely basis with the staff proposed accounting treatments for, or disclosures about, transactions or events that are not specifically covered by the existing accounting literature.

Footnotes

-[1]- American Institute of Certified Public Accountants ("AICPA"), Codification of Statements on Auditing Standards ("AU") § 312, "Audit Risk and Materiality in Conducting an Audit," states that the auditor should consider audit risk and materiality both in (a) planning and setting the scope for the audit and (b) evaluating whether the financial statements taken as a whole are fairly presented in all material respects in conformity with generally accepted accounting principles. The purpose of this Staff Accounting Bulletin ("SAB") is to provide guidance to financial management and independent auditors with respect to the evaluation of the materiality of misstatements that are identified in the audit process or preparation of the financial statements (i.e., (b) above). This SAB is not intended to provide definitive guidance for assessing "materiality" in other contexts, such as evaluations of auditor independence, as other factors may apply. There may be other rules that address financial presentation. See, e.g., Rule 2a-4, 17 CFR 270.2a-4, under the Investment Company Act of 1940.

-[2]- As used in this SAB, "misstatement" or "omission" refers to a financial statement assertion that would not be in conformity with GAAP.

-[3]- FASB, Statement of Financial Accounting Concepts No. 2, Qualitative Characteristics of Accounting Information ("Concepts Statement No. 2"), 132 (1980). See also Concepts Statement No. 2, Glossary of Terms–Materiality.

-[4]- TSC Industries v. Northway, Inc., 426 U.S. 438, 449 (1976). See also Basic, Inc. v. Levinson, 485 U.S. 224 (1988). As the Supreme Court has noted, determinations of materiality require "delicate assessments of the inferences a 'reasonable shareholder' would draw from a given set of facts and the significance of those inferences to him . . . ." TSC Industries, 426 U.S. at 450.

-[5]- See, e.g., Concepts Statement No. 2, 123-124; AU § 312.10 (". . . materiality judgments are made in light of surrounding circumstances and necessarily involve both quantitative and qualitative considerations."); AU § 312.34 ("Qualitative considerations also influence the auditor in reaching a conclusion as to whether misstatements are material."). As used in the accounting literature and in this SAB, "qualitative" materiality refers to the surrounding circumstances that inform an investor's evaluation of financial statement entries. Whether events may be material to investors for non-financial reasons is a matter not addressed by this SAB.

-[6]- See, e.g., Rule 1-02(o) of Regulation S-X, 17 CFR 210.1-02(o), Rule 405 of Regulation C, 17 CFR 230.405, and Rule 12b-2, 17 CFR 240.12b-2; AU §§ 312.10-.11, 317.13, 411.04 n. 1, and 508.36; In re Kidder Peabody Securities Litigation, 10 F. Supp. 2d 398 (S.D.N.Y. 1998); Parnes v. Gateway 2000, Inc., 122 F.3d 539 (8th Cir. 1997); In re Westinghouse Securities Litigation, 90 F.3d 696 (3d Cir. 1996); In the Matter of W.R. Grace & Co., Accounting and Auditing Enforcement Release No. ("AAER") 1140 (June 30, 1999); In the Matter of Eugene Gaughan, AAER 1141 (June 30, 1999); In the Matter of Thomas Scanlon, AAER 1142 (June 30, 1999); and In re Sensormatic Electronics Corporation, Sec. Act Rel. No. 7518 (March 25, 1998).

-[7]- Concepts Statement No. 2, 131 (1980).

-[8]- Concepts Statement No. 2, 131 and 166.

-[9]- Concepts Statement No. 2, 167.

-[10]- Concepts Statement No. 2, 168-69.

-[11]- Concepts Statement No. 2, 170.

-[12]- Concepts Statement No. 2, 125.

-[13]- AU § 312.11.

-[14]- As stated in Concepts Statement No. 2, 130:

> Another factor in materiality judgments is the degree of precision that is attainable in estimating the judgment item. The amount of deviation that is considered immaterial may increase as the attainable degree of precision decreases. For example, accounts payable usually can be estimated more accurately than can contingent liabilities arising from litigation or threats of it, and a deviation considered to be material in the first case may be quite trivial in the second.

This SAB is not intended to change current law or guidance in the accounting literature regarding accounting estimates. See, e.g., Accounting Principles Board Opinion No. 20, Accounting Changes 10, 11, 31-33 (July 1971).

-[15]- The staff understands that the Big Five Audit Materiality Task Force ("Task Force") was convened in March of 1998 and has made recommendations to the Auditing Standards Board including suggestions regarding communications with audit committees about unadjusted misstatements. See generally Big Five Audit Materiality Task Force, "Materiality in a Financial Statement Audit–Considering Qualitative Factors When Evaluating Audit Findings" (August 1998). The Task Force memorandum is available at www.aicpa.org.

-[16]- See Concepts Statement No. 2, 169.

-[17]- If management does not expect a significant market reaction, a misstatement still may be material and should be evaluated under the criteria discussed in this SAB.

-[18]- Intentional management of earnings and intentional misstatements, as used in this SAB, do not include insignificant errors and omissions that may occur in systems and recurring processes in the normal course of business. See notes 38 and 50 infra.

-[19]- Assessments of materiality should occur not only at year-end, but also during the preparation of each quarterly or interim financial statement. See, e.g., In the Matter of Venator Group, Inc., AAER 1049 (June 29, 1998).

-[20]- See, e.g., In the Matter of W.R. Grace & Co., AAER 1140 (June 30, 1999).

-[21]- AUI § 326.33.

-[22]- Id.

-[23]- The auditing literature notes that the "concept of materiality recognizes that some matters, either individually or in the aggregate, are important for fair presentation of financial statements in conformity with generally accepted accounting principles." AU § 312.03. See also AU § 312.04.

-[24]- AU § 312.34. Quantitative materiality assessments often are made by comparing adjustments to revenues, gross profit, pretax and net income, total assets, stockholders' equity, or individual line items in the financial statements. The particular items in the financial statements to be considered as a basis for the materiality determination depend on the proposed adjustment to be made and other factors, such as those identified in this SAB. For example, an adjustment to inventory that is immaterial to pretax income or net income may be material to the financial statements because it may affect a working capital ratio or cause the registrant to be in default of loan covenants.

-[25]- AU § 508.36.

-[26]- AU § 312.34

-[27]- AU § 380.09.

-[28]- FASB Statements of Financial Accounting Standards ("Standards" or "Statements") generally provide that "[t]he provisions of this Statement need not be applied to immaterial items." This SAB is consistent with that provision of the Statements. In theory, this language is subject to the interpretation that the registrant is free intentionally to set forth immaterial items in financial statements in a manner that plainly would be contrary to GAAP if the misstatement were material. The staff believes that the FASB did not intend this result.

-[29]- 15 U.S.C. §§ 78m(b)(2)-(7).

-[30]- 15 U.S.C. § 78l.

-[31]- 15 U.S.C. § 78o(d).

-[32]- Criminal liability may be imposed if a person knowingly circumvents or knowingly fails to implement a system of internal accounting controls or knowingly falsifies books, records or accounts. 15 U.S.C. §§ 78m(4) and (5). See also Rule 13b2-1 under the Exchange Act, 17 CFR 240.13b2-1, which states, "No person shall, directly or indirectly, falsify or cause to be falsified, any book, record or account subject to Section 13(b)(2)(A) of the Securities Exchange Act."

-[33]- 15 U.S.C. § 78m(b)(7). The books and records provisions of section 13(b) of the Exchange Act originally were passed as part of the Foreign Corrupt Practices Act ("FCPA"). In the conference committee report regarding the 1988 amendments to the FCPA, the committee stated,

> The conference committee adopted the prudent man qualification in order to clarify that the current standard does not connote an unrealistic degree of exactitude or precision. The concept of reasonableness of necessity contemplates the weighing of a number of relevant factors, including the costs of compliance.

Cong. Rec. H2116 (daily ed. April 20, 1988).

-[34]- So far as the staff is aware, there is only one judicial decision that discusses Section 13(b)(2) of the Exchange Act in any detail, SEC v. World-Wide Coin Investments, Ltd., 567 F. Supp. 724 (N.D. Ga. 1983), and the courts generally have found that no private right of action exists under the accounting and books and records provisions of the Exchange Act. See e.g., Lamb v. Phillip Morris Inc., 915 F.2d 1024 (6th Cir. 1990) and JS Service Center Corporation v. General Electric Technical Services Company, 937 F. Supp. 216 (S.D.N.Y. 1996).

-[35]- The Commission adopted the address as a formal statement of policy in Securities Exchange Act Release No. 17500 (January 29, 1981), 46 FR 11544 (February 9, 1981), 21 SEC Docket 1466 (February 10, 1981).

-[36]- Id. at 46 FR 11546.

-[37]- Id.

-[38]- For example, the conference report regarding the 1988 amendments to the FCPA stated,

> The Conferees intend to codify current Securities and Exchange Commission (SEC) enforcement policy that penalties not be imposed for insignificant or technical infractions or inadvertent conduct. The amendment adopted by the Conferees [Section 13(b)(4)] accomplishes this by providing that criminal penalties shall not be imposed for failing to comply with the FCPA's books and records or accounting provisions. This provision [Section 13(b)(5)] is meant to ensure that criminal penalties would be imposed where acts of commission or omission in keeping books or records or administering accounting controls have the purpose of falsifying books, records or accounts, or of circumventing the accounting controls set forth in the Act. This would include the deliberate falsification of books and records and other conduct calculated to evade the internal accounting controls requirement.

Cong. Rec. H2115 (daily ed. April 20, 1988).

-[39]- As Chairman Williams noted with respect to the internal control provisions of the FCPA, "[t]housands of dollars ordinarily should not be spent conserving hundreds." 46 FR 11546.

-[40]- Id., at 11547.

-[41]- Section 10A(f) defines, for purposes of Section 10A, an "illegal act" as "an act or omission that violates any law, or any rule or regulation having the force of law." This is broader than the definition of an "illegal act" in AU § 317.02, which states, "Illegal acts by clients do not include personal misconduct by the entity's personnel unrelated to their business activities."

-[42]- AU § 316.04. See also AU § 316.03. An unintentional illegal act triggers the same procedures and considerations by the auditor as a fraudulent misstatement if the illegal act has a direct and material effect on the financial statements. See AU §§ 110 n. 1, 316 n. 1, 317.05 and 317.07. Although distinguishing between intentional and unintentional misstatements is often difficult, the auditor must plan and perform the audit to obtain reasonable assurance that the financial statements are free of material misstatements in either case. See AU § 316 note 3.

-[43]- AU § 316.04. Although the auditor is not required to plan or perform the audit to detect misstatements that are immaterial to the financial statements, SAS 82 requires the auditor to evaluate several fraud "risk factors" that may bring such misstatements to his or her attention. For example, an analysis of fraud risk factors under SAS 82 must include, among other things, consideration of management's interest in maintaining or increasing the registrant's stock price or earnings trend through the use of unusually aggressive accounting practices, whether management has a practice of committing to analysts or others that it will achieve unduly aggressive or clearly unrealistic forecasts, and the existence of assets, liabilities, revenues, or expenses based on significant estimates that involve unusually subjective judgments or uncertainties. See AU §§ 316.17a and .17c.

-[44]- AU §§ 316.34 and 316.35, in requiring the auditor to consider whether fraudulent misstatements are material, and in requiring differing responses depending on whether the misstatement is material, make clear that fraud can involve immaterial misstatements. Indeed, a misstatement can be "inconsequential" and still involve fraud.

Under SAS 82, assessing whether misstatements due to fraud are material to the financial statements is a "cumulative process" that should occur both during and at the completion of the audit. SAS 82 further states that this accumulation is primarily a "qualitative matter" based on the auditor's judgment. AU § 316.33. The staff believes that in making these assessments, management and auditors should refer to the discussion in Part 1 of this SAB.

-[45]- AU §§ 316.34 and 316.36. Auditors should document their determinations in accordance with AU §§ 316.37, 319.57, 339, and other appropriate sections.

-[46]- See, e.g., AU § 316.39.

-[47]- Report of the National Commission on Fraudulent Financial Reporting at 32 (October 1987). See also Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (February 8, 1999).

-[48]- AU § 325.02. See also AU § 380.09, which, in discussing matters to be communicated by the auditor to the audit committee, states,

> The auditor should inform the audit committee about adjustments arising from the audit that could, in his judgment, either individually or in the aggregate, have a significant effect on the entity's financial reporting process. For purposes of this section, an audit adjustment, whether or not recorded by the entity, is a proposed correction of the financial statements . . . .

-[49]- See AU § 411.05.

-[50]- The FASB Discussion Memorandum, Criteria for Determining Materiality, states that the financial accounting and reporting process considers that "a great deal of the time might be spent during the accounting process considering insignificant matters . . . . If presentations of financial information are to be prepared economically on a timely basis and presented in a concise intelligible form, the concept of materiality is crucial." This SAB is not intended to require that misstatements arising from insignificant errors and omissions (individually and in the aggregate) arising from the normal recurring accounting close processes, such as a clerical error or an adjustment for a missed accounts payable invoice, always be corrected, even if the error is identified in the audit process and known to management. Management and the auditor would need to consider the various factors described elsewhere in this SAB in assessing whether such misstatements are material, need to be corrected to comply with the FCPA, or trigger procedures under Section 10A of the Exchange Act. Because this SAB does not change current law or guidance in the accounting or auditing literature, adherence to the principles described in this SAB should not raise the costs associated with recordkeeping or with audits of financial statements.

Appendix A—

Fraud Sector-By-Sector

1 CONSTRUCTION

1.1 Introduction

The construction sector includes entities conducting the following kinds of operations:

- Residential and commercial building construction
- Construction of roads, bridges and similar public works
- Residential and commercial renovations
- Installation of plumbing, electrical and similar infrastructure

This sector is highly cyclical, and competition for work can be fierce. The competitive pressure affecting construction firms, their employees, and sub-contractors can result in an increased risk of fraud.

1.2 Key Vulnerabilities

Some of the key vulnerabilities to fraud in this sector include:

- Contract bidding fraud (bid rigging, kickbacks, secret commissions and so on): Competitive pressures can lead to collusion among bidders on a contract, thus exposing the company to criminal prosecution. Alternatively, managers and employees who feel they have little stake in the company may accept kickbacks or secret commissions from either the company's customers or its suppliers in exchange for under-the-table financial consideration or preferential treatment.
- Materials substitution: Subcontractors may substitute materials of lower quality than called for in the contract specifications, in order to (1) make a profit on contracts they have underbid on, or (2) increase their profits. The company itself may also engage in this practice, exposing itself to criminal prosecution or civil liability.
- Tax evasion (underground economy): Especially in residential construction and renovations, companies may solicit or accept "cash-without-a-receipt" business, in order to avoid sales taxes as well as reduce their income taxes.
- Employee misbehavior (theft, sabotage, and the like.): Depending on the nature of the employee-employer relationship and the construction contract, some employees may feel little loyalty to the projects they work on and have no inclination to complete work on time. Line employees may steal materials or intentionally create time and cost overruns to extend their own employment. As material and labor costs soar during the construction phase, support personnel (for example, accounting or purchasing) may concoct inventory or accounts payable schemes to defraud their employer or customers.

1.3 Key Preventive Controls

Some of the key fraud prevention controls in the construction sector are described below.

- Corporate policies, particularly in the areas of employee relations and enforcement, are key to establishing an environment that minimizes the risk of fraud. If both management and lower-level employees feel they have a stake in the company and they also believe that (1) they are being fairly treated, for example with respect to compensation, and (2) any employee will be severely dealt with for any breach of the law or the company's policies, then they are less likely to engage in fraud, commercial crime or destructive acts.

- Physical access restrictions, for example with respect to construction materials and supplies at the company's premises and at work sites, will deter theft or sabotage.
- Supervisory performance and independent checks will help ensure that the company's work is up to contract standards and minimize the potential for materials substitution or other quality problems.
- Adequate insurance is especially important in this sector.

1.4 Checklist and Grids

A fraud risk management checklist specific to the construction sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Construction Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the construction sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Inventory fraud, such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, audit [especially confirmations], and supervision)	☐	☐	☐	___
• Secret commissions, kickbacks, etc. (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Sabotage and espionage by employees, competitors, or others (related controls include physical access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___
• Outsider frauds such as inflated supplier invoices or product substitution (related controls include good corporate policies and supervision)	☐	☐	☐	___
• Commercial crime by the organization, including environmental crime, tax evasion, and violating occupational health and safety laws (related controls include good corporate policies [especially strict enforcement and supervision] and strong internal, audit functions)	☐	☐	☐	___
• Other key risk management issues for this sector: insurance	☐	☐	☐	___

(continued)

CONSTRUCTION SECTOR CHECKLIST *(continued)*

Construction Sector Checklist	Yes	No	NA	Ref
b. Have the following vulnerability areas for the construction sector, and related controls, as set out on the attached grids, been adequately addressed: • Lapping frauds, such as accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies, especially strict enforcement)	☐	☐	☐	___

Fraud Vulnerability Grid Construction Sector	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers or credits)		X	
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)	X		
Payroll frauds (for example, ghost employees)	X		
Inflated expense reports by managers and others		X	
Bid-rigging, kickbacks, secret commissions, and the like	X		
Manipulation of financial statements by officers			X
Manipulation of share prices by directors and officers			X
Employee sabotage or espionage	X		
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (for example, inflated invoices, product substitution)	X		
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)			X
Environmental crime (for example, dumping)	X		
False advertising		X	
Insider trading			X
Money laundering		X	
Organizational bribe giving	X		
Tax evasion	X		
Violating occupational health and safety laws	X		
Violation of privacy			X

(continued)

FRAUD VULNERABILITY GRID—CONSTRUCTION SECTOR *(continued)*

Fraud Vulnerability Grid Construction Sector	High	Avg	Low or NA
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)	X		
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like		X	
Mandatory annual vacations			X
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both		X	
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both	X		
Supervisor follow-up (for example, exceptions, customer complaints)		X	
Auditors (internal, external)		X	
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)	X		

2 Financial Services

2.1 Introduction

The extremely high liquid asset values of the financial-services industry when coupled with the worldwide scope of its activities make it a prime target for fraud, from both inside and outside. Indeed, Willie Sutton, the infamous bank robber, probably summed it up best when he was asked why he robbed banks. He responded: "Because that's where the money is, stupid."

Customers of this industry's services are located throughout the world. Today, they can access its services through the mail, the Internet, the telephone, and finally, the traditional means, personally. Everyone, from small savers using their local bank's ATM to multinational conglomerates taking part in billion dollar mergers, requires this sector's services and products.

As a target for the fraudster, the financial-services industry is probably the richest and most rewarding target there is. Therefore, there is a pressing need to ensure that adequate internal controls are in place to deter and, when applicable, detect fraud on a timely basis. This must be properly appreciated and addressed by the financial service entities' managements, auditing and consulting CPAs, and customers.

For our purposes, the financial-services sector includes the following lines of business:

1. Banks (of all types including trust companies), and credit unions.
2. Insurance companies and insurance brokers.
3. Securities brokers (regardless of the type of investment or regulatory agency).
4. Mutual funds and retirement trust funds (including pension funds, 401ks and the like).

Although there may be a generally accepted perception that these entities are regulated by government agencies, the level of official oversight varies greatly. Further, that oversight is usually aimed at the solvency of the service entity itself, rather than whether an employee of an entity or an entity's customer is a fraudster. Therefore, neither the entities nor their customers can afford complacency or carelessness.

The fraudster, relying on personal knowledge of what the oversight agencies regulate and the controls that management has put in place, hatches his or her scheme to minimize the risk of apprehension by avoiding those very controls. Yet, the fraudster proceeds with his or her plan notwithstanding the general deterrence of criminal and civil laws. They know what they are doing is wrong, but they do it anyway.

Moreover, the deregulation of the financial-services industry has lead to the creation of super entities. Banks, insurance companies, investment brokers, and mutual funds are no longer separate entities. They are complete financial-services entities providing one or more services, all designed to provide their customers one-stop shopping. Unfortunately, the resulting financial behemoths could become too large to be effectively monitored by the same regulators and internal control systems that previously oversaw smaller, less diversified entities. This consolidation has facilitated the entry of the fraudster into the doors and portals of the industry and has provided increased opportunities for the fraudster to succeed. Incursions and fraudulent activity will likely become more widespread, more remunerative, and more difficult to track down.

Therefore, CPAs, both internal and external, and managements of the financial-services entities must actively develop and refine their systems of fraud prevention. They have to keep in mind Willie Sutton's observation; they are where the money is. They also must keep the special risks inherent to the financial-services sector in the forefront of their thinking. There is no gain to be made through profitable transactions if those profits are flushed down unknown drains.

Well designed and diligently implemented internal control systems should provide a special deterrence against the peculiar and prevalent types of fraud affecting the financial-services sector. As previously noted, the fraudster chooses to target the easy mark without fear of the law. Making it harder for him or her to operate can only serve to plug the drain.

The following material, drawn from actual case experience endemic to financial-services entities, summarizes and illustrates the kinds of fraudulent behavior to expect. These frauds highlight the sector's key vulnerabilities that are summarized and addressed by specific recommendations and controls found in the Checklist and Grids.

2.2 Key Vulnerabilities

The financial-services sector is subject to fraud by a wide range of perpetrators. Those most frequently encountered include:

- Employees. These frauds typically involve cash or accounts receivable. They range from outright theft or skimming of cash to the setting up of phony customer accounts. For example, some of the largest bank frauds have involved loan managers who set up phony borrowers and diverted the loan proceeds to their own benefit.
- Customers. Banks are vulnerable to customer-perpetrated fraud schemes, such as check kiting, credit-card/debit-card fraud, and phony loan security. Insurance companies are particularly vulnerable to fake or inflated loss claims by their policyholders.
- Con artists. This wily group of individuals sees this sector as having deep pockets and targets it with a wide variety of schemes, both direct and indirect. An example of a direct fraud scheme is one in which a bank loan manager is approached with an elaborate, seemingly irresistible short-term loan opportunity that would yield a quick profit. The catch is that, in addition to the proposal being totally fraudulent, the loan manager has to put up a large amount of bank funds for a short period of time. An example of an indirect fraud scheme is the, so-called, bank *inspector fraud,* in which a bank's elderly customer is persuaded by the con artist to help in the investigation of a teller. The catch is that the customer must withdraw a large amount of cash to further the con artist's phony investigation.
- Computers. The new tool of the fraudster. Hacking into other peoples' accounts or setting up fake transactions to net dollars is among the rapidly increasing number of computer frauds that are showing up. The fraudster is relying on the sector's heavy use of automation and its inability to look at all transactions to provide the time needed to grab the money and run.
- Breach of trust and related fiduciary activities: Fiduciary frauds include many types of commercial crime; for example, a stock broker or money manager could abscond with

a client's funds or churn a client's discretionary account with a series of unauthorized transactions to increase commissions; money laundering; or invasion of privacy for gain.

Banks (of all Types Including Trust Companies), and Credit Unions

Banks (of all types including trust companies)[1], and to a lesser extent credit unions, occupy a special niche in our society. They are allowed to engage in both the receipt of deposits and the lending of money. These cash-related activities offer numerous opportunities to the fraudster, both internal and external to the organization.

A cause of concern for entities acting in a fiduciary capacity is the potential for fraud through abuse of the relationship between a bank's subsidiary acting as an investment adviser and an investment vehicle, for example, a mutual fund sponsored and managed by a different subsidiary of the bank. Although underlying trust documents impose a fiduciary obligation on the bank as trustee to act in the best interest of the trust beneficiary, individual officers may favor bank-sponsored investments to bolster their personal careers to the detriment of the trust beneficiaries. Thus, internal relationships that induce, especially through financial remuneration, the bank to disregard its own fiduciary obligation may, depending on all of the attendant circumstances, lead to fraud. This is especially true when there are willful failures to disclose possible conflicts of interest, as happened with several banks implying to their customers that the *pure* investment products they were selling were insured deposits. For a further discussion of this topic, see the section below on mutual and pension funds.

Loan security is another bank vulnerability to fraud. Whether it is the loan applicant providing collateral that is not what it purports to be or a loan officer knowingly accepting insufficient collateral to show improved personal business, the potential for internal or external fraud exists. If the loan is large enough and the collateral rotten enough, a bank's very financial stability could be threatened.

Collateral Can't Be In Two Places At the Same Time Case Study

A bank sought to extend a substantial loan to a company in the precious-metals industry. The company dutifully completed all of the forms, including granting a security interest in its inventory of gold bars (bullion) to the bank. Following established good practices, the bank obtained the right to periodically audit and inspect the company's inventory records and underlying inventory. Every three months or so, the bank would send its internal audit team to check on its gold bullion. On Friday, the team would visit a vault in South America and record the presence of the hypothecated bullion. On Monday, the team would visit the vault in New York City and again record the presence of the requisite gold horde. Although the same gold bullion could not be in two different places at the same time, it was discovered that the same gold bullion somehow managed to be in two different places at two different times–just like the audit team!

---

[1] For the purposes of this analysis, *bank* includes commercial banks, savings banks, trust companies, credit unions and the like. There are important distinctions; for example, the agencies providing deposit insurance are not of importance to this discussion of fraudulent behavior.

Common sense and the willingness to devote adequate resources to important tasks such as the verification of collateral are essential. The bank's internal auditors failed to take those steps that should normally be followed by a reasonable CPA providing assurance services. For instance, the audits followed a recognizable pattern: South America followed by New York, never the reverse; and the audits were always sequential, never simultaneous.

Although there were probably other audit failings, such as giving the borrower advance notice of the audit, the bank's internal auditors had to establish a valid audit program to assure the continued existence of the gold. A further open door to fraud was the bank's failure to take possession of the collateralized gold in escrow. With the gold in its possession, the bank would be secure in its loan and its customer would have been able to use the bullion for its own business purposes, but with the bank's knowledge and approval.

Collateral Must Exist To Be Collateral Case Study

A frozen-seafood distributor obtained a loan from a bank using its frozen-seafood inventory as collateral. The bank properly executed all the normal collateralization documents, including the right to inspect the inventory and value its existence. Consistent with industry custom, the value of the collateral was indirectly related to its age; that is, the value of the seafood substantially decreased as it aged in the freezer.

Every three or four months, the bank would courteously call the seafood company, and obtain a mutually convenient date on which the bank's inspectors could inspect and value the seafood inventory. Once notified of the impending audit, the seafood company's employees would change the dates on the inventory in the freezers, making the old fresh and ever more valuable to the casual inspector.

In fact, the seafood company had been experiencing financial difficulties for a long time. Sales were slow, and working capital was short. In brief, the company could not afford to purchase new inventory.

The bank's inspectors were more than polite. They also did not like to spend time in the subzero temperatures inside the company's freezers. After entering the cold storage area, they would quickly check the dates of the boxes—labeled sea scallops, count a few, and then perform rough estimates of value.

There are highly tasteful meals that could be made of frozen sea scallops: They could be sautéed in garlic and olive oil and placed on a bed of saffron rice. This company's product, although labeled sea scallops, was actually detritus—inedible filler. The only proper place for this collateral was in a landfill. As security, it cost the bank more to haul it away than it would have fetched at market.

Among the lessons to be learned from this case are: know your customer, know your customer's product, go beyond the label on the package, and in all cases follow established inventory audit practices. Failure to have the recognized reasonable controls in place can only open the door wide for the external or internal fraudster.

Insurance Companies and Insurance Brokers

The insurance industry, which is an integral part of both the commercial and personal economy, is made up of three overlapping discrete functions. First, there are the insurance companies themselves (including reinsurance companies). They accept the risk of loss of others, whether it be for accidents, earthquakes, injury or death. Then the brokerage sector sells the product of the insurance companies to the world. Last is the claims function that determines the validity and value of the loss claims, and whether or not the claim is actually covered by the contract of insurance.

There is no uniformity in the insurance industry. Some insurance companies are totally integrated. That is, all three functions are under one roof: underwriting, sales and claims adjusting are all handled by the insurance company's employees. Other insurance companies "farm out" either the sales or adjustment functions to independent entities. Further, these independent entities might contract to work exclusively for one insurance company or agree to service a single insurance company.

Regardless of the structure, the same fraud opportunities, whether internal or external, exist. However, as in any other industry, the effectiveness of the insurance policy and its initiating sales step and subsequent potential for claims relies on the good-faith relationship between the parties involved.

Reliance on good faith, however, is no deterrence for the fraudster. Sufficient internal controls to make it difficult for the fraudster should be in place. Procedures at the insurance company level as basic as randomly verifying application information or validity of claims are needed (for example, was there really a hurricane on the date claimed?). Likewise at the brokerage level there should also be controls in place to ensure that the application information is valid. For instance, is the gray-haired, palsied applicant for a life insurance policy really the macho 45-year old he claims to be? Or, for a claims department, is there a methodology in place to determine that one doctor's name is showing up on an inordinate number of auto-accident injury claims?

At the same time, the customer of the insurance companies and its sales and claims functions have to be aware of the frauds they could be subjected to. The simple step of making sure that a company-issued contract of insurance is in hand will go a long way to protect against sales fraud. In addition, it is important to check that any repairs to damaged property are completed according to the terms of the insurance contract.

When Good Faith Becomes Bad Business Case Study

The ABC Company, a small start-up company, presents an interesting study of reliance on good faith. ABC began operations as a small manufacturer of specialized electronic parts for the defense industry. Due to good fortune and hard work, ABC grew. It had always used the services of a particular insurance broker, relying on it for all of the company's and its principals' insurance needs. Because there had been no problems with the coverage or the service, there was no reason for ABC to question the insured-broker relationship and certainly no reason to change brokers. For years, premiums were dutifully sent to the broker, and the broker routinely sent broker-generated confirmations of insurance coverage to the insured.

Unfortunately, the familiar maxim "you don't know whether your basement takes in water until it rains hard" was applicable in this instance. A terrible storm engulfed the area. Many businesses and residences were devastated. Buildings, equipment, and inventory were destroyed, including over a million dollars' worth of property damage to ABC.

"Thank God for the insurance," exclaimed the principals of ABC. Unfortunately, God was likely their best recourse. The long-trusted, premium-accumulating insurance broker had discovered that there are warm and sunny places on the earth where the long arms of the U.S. justice systems do not reach. What better place to take all of those diverted premiums? The ABC Company discovered the hard way that trust is like water. Some is essential to prevent dehydration; however, too much will drown you. A simple, regular review of the insurance file to confirm the presence of company-issued documents of valid insurance would have been sufficient to avoid the loss.

The moral of this story: don't accept the assurance of your insurance intermediary–your broker–confirm that he or she spent your money with the insurance carrier; look for the carrier-issued policy for verification.

Because this failure to pay over premiums was such a common occurrence, a limited amount of the risk was shifted to the insurance companies. If a supposed insured can prove payment of a premium to a fraudulent broker or agent, there is some limited degree of protection. This is designed to help the unsophisticated consumer. ABC's losses would have far exceeded any industry or government-ordered protection.

Up in Smoke and Into Thin Air Case Study

In this case, the insurer was the deceived party. A New York City company, which had a valid fire insurance policy covering structure and inventory, lost most of its inventory in a warehouse fire. Unfortunately, the records proving the existence of the inventory were also destroyed in the fire. The insurer quickly discovered that you don't necessarily know what you have until it's gone, even if it was never really there.

The insured prepared a million-dollar-plus claim for the lost inventory, notwithstanding the absence of records and despite the existence of some eye-opening circumstances. Here are the obvious clues that all was not right with the claim:

- First: the claimed value of the inventory was nearly three times the value of the preceding year's inventory. Was the company apparently anticipating an unprecedented rush of sales or did it have an unexpected growth spurt?

- Second: the non-financial records, including personnel files and insurance policies, were removed from the warehouse office two weeks before the fire. The financial records were the only records left in the office.
- Third: the insured tripled the insurance policy coverage on the last policy renewal date one month prior to the fire. Was this the reasonable forward-looking planning of a profitable business or, in hindsight, the planning of an unprofitable business?
- Fourth: in support of its proof of damages, the insured offered a valuation of the company, including its inventory, dated less than two months before the fire. The valuation was prepared for the owner as part of an apparently contentious divorce proceeding with his estranged wife, who alleged that the owner had incurred huge gambling debts.

  The valuation was not credible, however, because it was tainted by irremediable bias. Investigation revealed that the valuator and owner were brothers. In actual fact, the only financial circumstance that could be verified was the owner's $100,000 payment to his brother, the valuator, for his fictitious valuation from which both spouses hoped to reap a bonanza at the insurance company's expense.
- Fifth: the insured confirmed the suspicions of investigators when a fully-prepared claim was submitted less than two weeks after the fire.

Clearly, foresight is superior to hindsight; in this case the insured party was far too well prepared. And the foresight of the insurance carrier to have the controls in place to allow the recognition of the false claim illustrates that superiority of foresight.

Cooking the Books Case Study

The construction industry is one of the most cyclical and seasonal. These expected irregularities can threaten or impair a construction company's ability to secure surety bonding, a requirement necessary to bid for and obtain work. Pursuant to a surety company's demand, the construction company requested its independent auditor, a CPA firm, to issue a report on the company's financial statements for the preceding year. The construction company's management and the CPA firm's audit engagement partner foresaw some difficulties. The year in question was not a good year for the company.

Business can be complicated. Thus, cooperation can be the foundation of success for many ventures. Over the course of many years, the CPA firm had grown dependent on the revenues received from its audits of the construction company. In fact, the construction company was its best client.

The construction company management and the audit engagement partner agreed that: the end justified the means. Besides, liberties, although improper, could be taken with GAAP; there was apparent flexibility. Given the circumstances, the company's method, with the complicity of the auditor, of obtaining the bonding did not seem relevant. Further, the auditor rationalized that it wasn't as though the company couldn't do the job.

In furtherance of the scheme, the company and the audit partner conspired to prepare and issue fraudulent financial statements. Inevitably, Murphy's Law (that which will go wrong, will in fact go wrong) struck and the company, with a dire shortage of working capital, defaulted on the job.

After the default the surety smelled a rat. Unfortunately, for the surety company, it took the work of independent forensic accountants with an in-depth knowledge of the construction industry to unravel and expose the deliberate falsity of the financial statements. The surety, in relying exclusively on the company and its CPA firm, did not perform its own due diligence.

A simple step, such as independently verifying bank accounts would have saved the surety big bucks. Clearly, an ounce of prevention is worth a pound of cure.

Stock and Other Investment Brokers

With so much wealth invested under the custody of stock and other investment brokers, clients of the investment-brokerage industry need to keep a vigilant watch on their investments (and therefore their money). Notwithstanding the general observation that most brokerage activities are perfectly legitimate, fraudulent activity does occur both within the inner workings of the industry and externally.

Internal fraud in the securities markets usually involves complex transactions, such as illegally parking stocks and undisclosed trading on insider information for illicit personal gain. Externally, the foisting of fraudulent investments on unsophisticated investors, who are only too ready to put their money in investments that are too good to be true, is all too common.

Exceptional circumstances organized or exploited by fraudsters may wreak financial devastation on swindled clients. Often, fraud in the brokerage industry results from an omission to disclose material information or an intentional misstatement of a material fact. The fraudster manipulatively preys on greed, gullibility, and an unwillingness to look behind the fraudster's spiel. Getting the rich to part with their money is an art to which some fraudsters dedicate years.

If It Looks Too Good To Be True... Case Study

A prominent couple in a New Jersey suburb had savings to invest. The husband had been the mayor of his medium-sized town for eight years. The wife worked for many years as a manager for a major insurance carrier in the same town. Arguably, the husband and wife were reasonably sophisticated. Then they threw a party.

Friends invited friends and the couple made new acquaintances, including a well-dressed, well-spoken, gentleman who worked for a small but apparently successful brokerage firm in Connecticut. The couple had not heard of this brokerage, but they had known their mutual friend for nearly two decades. What better reference would they need other than the word-of-mouth assurance from their trusted friend?

The broker recommended a hot new investment: limited-partnership interests in oil and gas properties off the coast of China. These investments were hot and availability was selectively limited, so the broker urged the couple to act quickly or risk being frozen out of the offering.

To be part of the buying syndicate, the couple had to put $200,000 up-front immediately. They knew that they should wait for the prospectus but they were afraid the delay could mean the possibility of losing the opportunity to put their money into this sure-fire investment. So rather than wait, the couple transferred the requested funds to the broker, and in due course they received papers verifying their investment. For eighteen months the couple received a monthly statement showing the value of their investment in the limited-partnership interests. It was a good investment, or at least it seemed so on paper.

After two months passed without a statement, however, the couple called the broker, using the telephone number on the earlier months' statements. The telephone company informed them that the number was no longer in service.

Further inquiry revealed the following:

- The limited partnerships never existed in economic reality.
- The brokerage had no employees other than their friend's friend.
- Neither the brokerage nor its sole employee was registered at the state or federal level to sell securities.
- The only asset owned or held by the brokerage was a computer with a high-quality printer.

What went wrong here? Quite simply, the fraudster, posing as an investment broker, was working on the principle that you can't fool all of the people all of the time, but you can fool some of the people some of the time. Especially if greed is involved.

It is foolish for anyone to think that he or she is immune from being prey to such tactics. It takes a wise person to recognize that anyone can be deceived, particularly if there is pressure based on the importance of acting quickly—no need to perform your normal due diligence, you know I'm legit—and greed—returns like this don't come along every day—are permitted to override reason. Wearing an expensive suit, flashing luxury jewelry, and displaying the confidence of a person who has profound familiarity with the capital markets are personal attributes that assure neither any return on investment nor a commitment to act with integrity.

Among other types of fraud perpetrated by unscrupulous brokers are unauthorized trading, churning, and market (price) manipulation. Occasionally, the compensation structure applicable to brokers serves to promote fraudulent conduct. Brokers whose income depends on commissions and bonuses based on the volume of trading generated by their clients are directly rewarded for the quantity and not the quality of trades they initiate on behalf of their clients. This suggests that clients should exercise careful scrutiny of their broker's conduct, especially when it comes to granting discretion to trade. Probably the best advice is: do not give unfettered trading discretion to a broker or investment adviser. Although the broker could be totally honest when the relationship begins, a change in circumstances brought about by events, such as losses at the racetrack or in the market, or unexpected heavy medical expenses at home, could change the situation. The potential temptation for fraud is always there.

Among the brokerage-related scams in vogue is a short-sellers' spreading of intentionally false and misleading information in an attempt to depress the value of a target company's publicly traded stock. This practice has become particularly prevalent on bulletin boards through the Internet. Of course, the victim here is not only the company but also investors who were duped into selling perfectly good stock for the wrong reason. Typically, in these cases the short-selling broker-dealer accumulates a substantial uncovered short position in the company's stock. Essentially, the broker-dealer sells borrowed stock; that is, stock that the broker-dealer is obligated to purchase in the future to apply against the uncovered short position.

In the case of the good-faith short-seller, he or she is speculating that the price in the target company's stock will drop for any number of valid market reasons, such as failure to meet earnings projections or the loss of a significant customer. Short selling is a valid and sound trading tactic. However, in the case of the bad faith short-seller, he or she is deliberately engaged in market manipulation for the purpose of depressing the target's stock price for personal gain. The fraudster posts rumors or tips on message boards warning of events, such as high-level management dissension or recent inquiry by the Federal Bureau of Investigation or some other such risk-raising circumstance. Often in these cases, investors cannot or will not engage in patient reasoning or exercising due diligence. The race goes to the swift, and the herd-mentality takes over, causing a deluge of sell orders, depressing the target company's stock price to the joy and personal enrichment of the fraudster.

Although this kind of fraud is relatively easy for the short seller to perpetrate in stocks with limited distribution, it is more difficult for widely held stocks. The new tool of the fraudster is the Internet. It provides the opportunity to widely distribute opinions, regardless of their validity. At the same time the Internet facilitates the fraudster's trading activities from the comfort of his or her home. As well, the Internet provides a certain degree of secrecy. There is a tendency by users to accept the information posted and the trades don't necessarily show up immediately in the normal source sites. It behooves the investor to be wary of and resist unfounded rumors and other misleading acts of market manipulation.

Mutual and Retirement Funds

The multi-billion-dollar value of investments in mutual and retirement funds presents a strong appeal for the fraudster. The mutual fund managers and retirement fund trustees as institutional investors have substantial market power and can command expert service, including research, from the securities industry. Moreover, the money in these funds often represents savings to be held for long-term investments for which custody has been given to a fiduciary, that is, fund manager or retirement plan trustee. While most situations involve reliable, competent administrators, it is always best to be aware of the pitfalls that can and do occur. Although no one can anticipate all of the acts of the fraudster, care should be taken to limit vulnerability and to maintain the flow of timely feedback. Few people are so busy that they can afford to lose hundreds of thousands of dollars. There is no substitute for vigilant monitoring of investments regardless of whether they are held in mutual funds, retirement plans or "long," that is, in the securities themselves.

Too Busy, Too Trusting, Too Bad Case Study

Occasionally, the lines of communication between mutual fund administrator and individual investors are subjected to malicious manipulation, often, as a result of the investors' own (misguided or erroneous) request. For instance, a well-respected mutual fund regularly mailed its monthly statements to its investors. One investor requested that his statements be mailed to his newly selected financial adviser, notifying the mutual fund that he was too busy to read them. At a later date, the adviser provided evidence of authority to act on behalf of the investor. Shortly thereafter, the adviser, without advising the client, liquidated the entire mutual fund investment, requesting that the proceeds be delivered to his address. The back-office of the mutual fund complied, not suspecting the fraudulent action of the adviser. Unfortunately, the financial adviser had no specific authority to order the complete redemption on behalf of the investor. The documentation provided to the mutual fund was bogus; the money disappeared into Nigeria. Worse, the investor did not discover this swindle until several months after the fact. He was too busy.

Generally, mutual funds provide a ready means of diversifying a portfolio without buying all the individual stocks (or bonds) held in the fund. Professionals, usually with verifiable records of performance, manage the funds. Regulatory monitoring is with the federal government (SEC), and some states offer additional regulation through their blue-sky laws. This monitoring does not, however, extend to the type or quality of the investments. Thus, the door is open for a mutual fund, notwithstanding management by professionals who should know better, to fall victim to fraudulent conduct. The competition to increase investment-return performance, which it is hoped will stimulate sales of the mutual fund, can lead to investments with a higher risk of fraud. For instance, investing in emerging nations could successfully yield high returns, but often the lack of regulation, lax enforcement of existing regulations, and different standards of business ethics lead to fraud-induced investment losses. The further afield the search for an investment takes the investment manager, the greater the risk of making an investment that is likely to fail as a result of fraud.

Gambling by Any Other Name Is Still Gambling Case Study

Some mutual fund managers are as willing to buy rosy but unrealistic prospects and forecasts as any other credulous investor. Returns from a manufacturing company based in the Commonwealth of Independent States (the former Soviet Union) were expected to increase dramatically. With privatization loosening the market and a large influx of capital from U.S. mutual fund investors, this business could not lose. It had made money under the rigid Soviet administration, so it stood to reason that it could only make more money given the application of Western capitalism.

Unfortunately, the economic model practiced by the business was crony capitalism. Only a fraction of the invested capital trickled down to the actual production, and the debts incurred by the rapid expansion wreaked havoc, inducing a significant restructuring in which millions of dollars were "lost."

Was this a fraud? Undoubtedly the application of principles of due diligence would have disclosed both the especially high risk of the investment and the extreme improbability of success. If the fund involved were advertised as a high-risk overseas fund, the purchasers were put on notice as to what they were buying into. The manager was following the investment objectives of the fund: high risk yields high returns. Probably not fraud unless the manager had knowledge before investing that the investment was itself a fraud.

If the fund was a large cap growth fund or some other moderate-risk fund, and the same investment were made, the answer would probably be different. For example, would the investment manager have invested his own funds in his moderate risk fund knowing of the investment in the high-risk former Soviet business? A high-risk investment might be said to be fraud or at the least negligence if the fund manager makes the investment in an effort to see a relatively staid fund beat modest market expectations and outperform the competition. Clearly, the manager strayed from the published investment goals of the fund. Although the professional manager's mindset may not have been fraudulent, his willingness to buy into the fraudulent scheme of the manufacturing company resulted in large losses for the fund.

There is a fine line. When does an act of investing become fraud? One obvious situation is the case of the investment manager who makes a suspect investment because of personal gain: as an inducement the subject company kicks back 10 percent of the investment to the manager off the books. Thus, investors have to monitor the investments of the funds to make sure they meet the fund's stated goals. Likewise, the senior administrators of the umbrella group of funds to which the individual fund belongs have to review their fund's investment manager's activities to see whether the investments the manager made match the fund's objectives, and if not, why?

Retirement plan funds are particularly vulnerable to fraud, breach of fiduciary duty, and other dishonest conduct perpetrated by the plan trustee, plan sponsor, or other persons responsible for investing these savings on the plan's behalf. This is because few persons monitor their own investments adequately. As with mutual funds, each investor's contribution is pooled with numerous other investors' contributions. The idea that somebody must be watching closely is widely—although mistakenly—held. After all, an employer (plan sponsor) would always make its contributions, wouldn't it?

Never a Borrower Be . . . Case Study

The business' profit margins were tight. Working capital was inadequate and the cost of capital prohibitive. As well, the limit on the line of credit had been exceeded. So, the business looked to the only source of ready cash it could find;` it "borrowed" from the pension fund. Just a little at first. A million here, a million there; soon, it became easy, almost a habit.

To avoid scrutiny of the business' CPAs who most certainly would have picked up on the new source of cash, the business' CFO and president conspired to get rid of the old CPA firm and hired a replacement CPA firm. Not surprisingly, the conspirators chose a small, understaffed, somewhat inexperienced CPA firm. The new CPA firm looked at the new engagement as a growth opportunity; it was an engagement that represented the lion's share of its billings. Disguising the *borrowings* as seemingly legitimate and independent private placements in the pension fund's financial statements, the business continued the fraud. However, earnings didn't pick up, things remained slow. "No sense in borrowing all that good money only to watch it disappear in the losing business, the fraudsters agreed; let's keep it ourselves."

The threat of the criminal justice system and expected integrity go only so far. They fall short sometimes, and the business also fell short for its employees. The business' creditors, who were also shortchanged, forced it into involuntarily bankruptcy.

Unraveling the fraud proved embarrassing. The employees, that is, the true investors in the retirement plan, had only the prison sentences of the malefactors and worthless orders of restitution as solace. With the principal players in jail and the money nowhere to be found, the employees have only the limited recovery that can be expected from the Pension Benefit Guaranty Corporation to replace their losses.

2.3 Key Preventative Controls

Because of the large asset values at stake, there are many fraud prevention controls in the financial-services sector that must be in place to effectively reduce the risk of fraud. At best, informed and watchful monitoring tends to deter the fraudster, chasing him or her elsewhere. Or if the fraudster decides to challenge the controls taxing his or her cleverness, the controls might induce an exposing mistake. At worst, the controls can make the fraudster even more ingenious than before.

Notwithstanding adequate controls, the world is not perfect. There are no guarantees; the fraudster will at times succeed. But the controls are a success if their effect is to make the fraudsters' successes fewer and less frequent.

- Remember that fraudsters will invent or exaggerate insurance claims, divert premiums, and otherwise take undue advantage of a given situation. Controls must be in place that will make it difficult and so challenging for the fraudster that he or she will shop elsewhere for an insurance broker or company. Verify details and research relationships. Do not assume that all lies will be small ones. This is not to suggest that insurance companies should erect insurmountable obstacles against all parties seeking payment on claims. No company employing reasonable compliance practices coupled with sound internal controls and plain common sense need sacrifice the goodwill of its policyholders.
- Mutual fund and retirement plan statements should be reviewed and read with understanding by all investors. This should be done as a matter of course shortly after the statements are received. Unless otherwise unavoidable, do not delegate this important activity to others, especially those who have access to the accounts. Do not

assume anyone will bear the burden without sticking his or her hand into the pot containing the funds.

- Ask questions about particular investments. At least make the plan sponsor and plan trustee aware that people are looking. Follow-up on potential red flags such as an unexplained or unexpected change in the independent CPA firm.
- Employees contributing to 401(k) plans should actively monitor their accounts. Track employer contributions on the statements periodically received from the trustee. At year end reconcile trustee's statements with the amounts shown on Form W-2 as having been deducted. In addition, verify that the investments have been placed into the proper funds. Understand what are the allowable investments, and understand what fees are proper.
- When selecting a broker for stock and other investments, clients should confirm that the broker is properly registered and is covered by the Securities Investor Protection Corporation (SIPC). The National Association of Securities Dealers (NASD), the North American Securities Administrators Association (NASAA), the Securities and Exchange Commission (SEC), state regulatory agencies, and the Federal Trade Commission are sources of information about the brokerage industry and individual brokers. Moreover, clients should carefully review the documentation supporting the client-broker relationship, including contracts and dispute procedures. In a continuing investment relationship, the client should promptly review transaction confirmations and monthly statements. If unauthorized trading or other misconduct is evident, immediately lodge a complaint with the brokerage's management. If this does not provide satisfaction, further steps, such as contacting the SEC or state authorities, should be taken without delay even if the unauthorized trade appeared to be a profitable investment decision for the client.
- Because product offerings are complex, clients should not overestimate their own level of competence. Some investments are suitable only for those who can afford large losses. Unfortunately, in a climate of volatile markets and sexy products, for example the class of product called derivatives, some clients let greed get the best of them, choosing to gamble rather than invest. The fraudster takes advantage of the get-rich-quick dream driven by greed. The potential for making an investment based on greed exists in everyone, and the sweet-talking fraudster is ready to exploit this human failing.
- In addition, it is essential that the following controls be put in place for all businesses within the financial-services sector:

  —A strong written code of ethics and well-defined business conduct should be mandatory for all employees. There should be sanctions for any employee who fails to adhere to these guidelines.

  —Effective physical access controls.

  —Thorough screening of employees prior to hiring. At a minimum this should include checking all references, including education and work history. Some organizations in this sector should go even farther, especially for more sensitive positions. This could include more extensive background checks, psychological testing and even drug testing.

  —Mandatory annual vacations of, at a minium, two consecutive weeks. Ongoing schemes are common in this sector. These schemes often fall apart or are easily detected when the perpetrator is removed from the scene for a consectutive period of even a few weeks.

—Prohibition of management override of basic controls. There have been many instances of branch managers in this sector who were able to circumvent or override basic controls. This power to override enablied them to perpetrate extremely large frauds sometimes running in the millions of dollars.

—Good computer security including access restrictions, disaster recovery contingencies and control over software and program development.

—Supervisory controls including a well-defined review and approval process, test-checking and monitoring of employee performance, and thorough follow-up of any exceptions or customer complaints.

—A strong internal audit function, and periodic external audits.

2.4 Checklist and Grids

A fraud risk management checklist specific to the financial services sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

(Text continued on page 11)

Financial Services Sector Checklist	**Yes**	**No**	**NA**	**Ref**
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the financial services sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Customer and other outsider frauds, such as false loan applications, con schemes, and the like (related controls include job descriptions and segregation of duties, supervision, good corporate policies, and strong internal audit function)	☐	☐	☐	___
• Commercial crime by the organization, including breach of trust, money laundering, and violation of privacy (related controls include good corporate policies [especially strict enforcement and supervision] and strong internal audit functions and periodic external audits	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___

Fraud Vulnerability Grid **Financial Services Sector**	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)	X		
Accounts receivable (for example, lapping, phony customers or credits)	X		
Inventory fraud (for example, theft, diversion)			X
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like		X	
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers		X	
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like	X		
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (sabotage, espionage, and the like)			X
Con schemes or extortion by outsiders	X		
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (theft of funds, misuse of information,and the like)	X		
Environmental crime (for example, dumping)			X
False advertising		X	
Insider trading		X	
Money laundering	X		
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety laws			X
Violation of privacy	X		

FRAUD VULNERABILITY GRID—FINANCIAL SERVICES SECTOR *(continued)*

Fraud Vulnerability Grid Financial Services Sector	High	Avg	Low or NA
Corporate Policies:			
Corporate mission statement and code of ethics	X		
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	
Fair performance appraisal and review system		X	
Employee screening and testing before hiring	X		
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like		X	
Mandatory annual vacations	X		
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both	X		
Prohibition of management override of controls	X		
Computer Controls:			
Access restrictions (for example, physical access, passwords)	X		
Regular off-site backups of programs and data files	X		
Software controls (for example, antivirus, full documentation)	X		
Programmer controls (for example, supervision, antisabotage)	X		
Supervisory, Internal-Audit Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval	X		
Supervisory performance, or independent checks, or both	X		
Supervisor follow-up (for example, exceptions, customer complaints)	X		
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

3 Government

3.1 Introduction

The government sector includes:

- Federal, state, and municipal governments.
- Government agencies and government-owned corporations.
- Organizations that receive most of their funding from government sources. For example, depending on the jurisdiction, this could include public elementary and seconday school systems; institutions of higher education (for example state university systems and local community colleges); municipal and state hospitals; and local ambulance services and volunteer fire departments.

Because of its tremendous size and the large budgets involved, this sector is especially prone to supplier and accounts payable frauds.

3.2 Key Vulnerabilities

Some of the key vulnerabilities to fraud in this sector include:

- Theft or diversion of government-owned inventory, for example office supplies.
- Accounts payable schemes by managers or employees, involving phony suppliers, inflated invoices, and so on.
- Overstated expense accounts.
- Acceptance of bribes (kickbacks, secret commissions) in exchange for contract approvals or inflated price approvals.
- Frauds by suppliers (overbilling, double-billing, product substitution, and so on).
- Computer-related fraud.
- Money laundering, for example, through government-run lotteries or pari-mutual betting facilities; bribe giving, for example through government-owned corporations or agencies seeking foreign sales.
- Violation of privacy, because of the extensive records on individuals kept by this sector.

Tax evasion is obviously also a major problem in this sector, with the perpetrator in this case being the taxpayer.

3.3 Key Preventive Controls

Some of the key fraud prevention controls in the government sector include:

- Strong enforcement, that is, ensuring that employees are severely dealt with for any breach of either the law or the government's policies.
- Good employee relations. This is especially important because of the large number of employees in this sector and the very high percentage who are unionized. Poor handling of this area can lead to a very antagonistic employer-employee relationship, which can not only lower productivity but also increase the risk of fraud, sabotage, and other illegal acts by some employees.

- Job descriptions that are clear and adhered to, including appropriate segregation of duties. For example, the responsibility for each step in the accounts payable cycle (such as contracts, requisition, purchase order, receiving, accounts payable, check preparation) should ideally be segregated to minimize the otherwise high potential for fraud in this cycle.
- Good computer security including access restrictions, disaster recovery contingencies, and control over software and program development. This is important not only to ensure smooth operations, but also to avoid breaches of confidentiality, or the misuse of information, or both.
- Supervisory controls including a well-defined review and approval process.
- A strong internal audit function.

3.4 Checklist and Grids

A fraud risk management checklist specific to the government sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Government Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the government sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees, and expense report fraud (related controls include job descriptions and segregation of duties, audit [especially confirmations], and supervision)	☐	☐	☐	___
• Secret commissions, kickbacks, etc. (related controls include job descriptions and segregation of duties, supervision, and good management policies [especially strict enforcement])	☐	☐	☐	___
• Inventory fraud such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good management policies [especially strict enforcement])	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___
• Outsider frauds such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good management policies and supervision)	☐	☐	☐	___
• Commercial crime by or against the government, including money laundering (for example, for government-run lotteries and pari-mutual betting operations), tax evasion, and violation of privacy (related controls include good management policies [especially strict enforcement and supervision], and strong internal audit functions [especially internal audit])	☐	☐	☐	___

(continued)

GOVERNMENT SECTOR CHECKLIST *(continued)*

Government Sector Checklist	Yes	No	NA	Ref
b. Have the following vulnerability areas for the government sector, and related controls, as set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good management policies [especially strict enforcement])	☐	☐	☐	___
• Sabotage and espionage by employees or others (related controls include physical access restrictions, and good management policies [particularly at the hiring stage])	☐	☐	☐	___

Fraud Vulnerability Grid Government Sector	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers or credits)		X	
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)	X		
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others	X		
Bid rigging, kickbacks, secret commissions, and the like	X		
Manipulation of financial statements by managers		X	
Employee sabotage or espionage		X	
External Frauds:			
Theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)	X		
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like.			X
Use of Computers in Fraud	X		
Commercial Crime:			
Breach of trust (theft of funds, misuse of information, and the like)			X
Environmental crime (for example, dumping)		X	
Money laundering (for example, lotteries and pari-mutual betting operations)	X		
Organizational bribe giving	X		
Tax evasion (that is, where the taxpayer is the perpetrator)	X		
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy	X		
Government Policies:			
Mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)	X		
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	

(continued)

FRAUD VULNERABILITY GRID—GOVERNMENT SECTOR *(continued)*

Fraud Vulnerability Grid Government Sector	High	Avg	Low or NA
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)		X	
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both			X
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)	X		
Regular off-site backups of programs and data files	X		
Software controls (for example, antivirus, full documentation)	X		
Programmer controls (for example, supervision, antisabotage)	X		
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval	X		
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)			X

4 HIGH TECHNOLOGY

4.1 Introduction

High technology is the constant process of technical innovation in every industry. However, the current use of what has become a modern everyday term usually refers to the fields of electronics, computers and other data processing equipment, telecommunications, biotechnology, defense and aerospace, and other related fields. The *Merriam Webster's Collegiate Dictionary* (Tenth Edition) defines high technology as, "the scientific technology involving the production or use of advanced or sophisticated devices esp. in the fields of electronics and computers." The common thread among the various definitions is always the latest or most recent technical advancement in a field or industry.

These technologies were made possible by the breakthroughs in mathematics, physics and biology of the 20th century. High technology is distinguished not only for the products that have increased the convenience and enjoyment of our lives but also for the revolutionary business strategies that have changed the way business entities think about management, markets and customers.

High technology is not an industry as such but is a means of digitizing information and managing processes that cut across all industries. Technology permits the improvement of manufacturing operations on the shop floor in addition to the flow of information in the front office. We identify high technology as the latest advancement and permutation in an industry that augments an existing process to the point of possible revolution.

For our purposes, we will focus on the possible frauds and controls in the high technology sector, which includes the following fields or industries:

1. Computer hardware and software development, installation and implementation
2. E-commerce and cyberfraud
3. Telecommunications
4. Biotechnology
5. Defense and aerospace
6. Other leading-edge scientific or industrial research and development

In addition, we will consider both the creation and use of this new technology in nonscientific or nontechnical areas. For example, many industries such as the automotive industry are a mixture of old and new technologies. A car is still four wheels on a frame but it also has a wide array of electronic equipment, from the automated voice that tells you your seatbelt is undone to the sensors that automatically adjust your speed relative to your proximity to adjacent vehicles.

What is common to high technology in all industries, however, is usually a new idea or product that could be very valuable on the open market for that industry. These products also carry high-risk levels, and major research and development expenditures to support them. Unfortunately, the presence of large funds and the bottomless appetite of a gullible public for new places to speculate with their money has attracted a new generation of fraudsters practicing many of the same old tricks and a few new ones. As always, big money attracts big crime. The fact that small companies have proliferated in this sector of the economy has attracted fraudsters who float new companies, take shareholders' money and disappear. The proprietary nature of much of the research has also raised the profile of the industrial spy. Getting the jump on the competition is essential when the financial stakes are so huge. Knowing who's doing what and when a competitor's new product is coming to market can mean life or death to a young startup living on a limited amount of venture capital.

4.2 Key Vulnerabilities

The primary key vulnerabilities to fraud in the high-technology sector include the following:

- Theft or diversion of inventory, for example, small items, such as computer chips, that have a high per-unit dollar value. In this area, the computer can be both the target of the fraud and used as the instrument to commit the fraud. The main vulnerability with new or leading-edge computer technology is the proprietary nature of the intellectual property involved in the product. The physical targeting of a computer is not limited to theft of its various components. The information stored on a hard drive of a targeted computer can be sold, especially if it contains important proprietary information, such as customer lists or prototype design information. Trafficking in counterfeit computer components is a major problem, especially with the many so-called *discount* merchants clamoring for the consumers' dollars. For instance, in once case a company was indicted on charges of trafficking in counterfeit CPU (Central Processing Unit) chips and software. Legitimate computer CPU manufacturers, such as Intel Corporation, qualify their CPUs to operate at specified speeds, mark that speed on the CPUs themselves, and further mark the CPU with their trademarks and other identifying information. To ensure the quality and life expectancy of the CPU, the legitimate manufacturer specifies each CPU to operate at less than top speed, and incorporates a speed-lock mechanism into each CPU to prevent operation at a speed greater than that specified.
- Counterfeiters, however, typically acquire genuine computer CPUs, remark them so that they will appear to be of superior quality and speed than they actually are, and disable the speed-lock mechanism. The counterfeiter then puts the mismarked CPUs in the supply chain through wholesalers, and in turn sells to retailers at steep discounts. The end consumer buys the inferior CPU, assuming it to be the genuine article with the expected superior quality and speed, at a price commensurate with the real thing. As a result, the purchasers are victimized because the remarked CPUs are more likely to burn out from ordinary use sooner than the properly adjusted legitimate ones. This results from the strain of operating at a higher speed than the true specification. So the consumer doesn't get what he or she thinks was paid for and the legitimate manufacturers are victimized by lost sales of their superior quality CPUs and the loss of faith in their genuine, quality products.
- Frauds by officers or directors, such as fraudulent financial reporting, stock touting, manipulation of share prices, insider trading, antitrust violations, or organizational bribes given as part of the contract bidding process.
- Sabotage and espionage, both from inside and outside the organization.
- Failure to communicate the potential security gaps to employees, businesses, and customers of the technology they use on a daily basis. This is especially true when interacting with the Internet.

- Failure of a company to install adequate security measures, properly maintain and update them, and to make the fact that they are in place known to system users, both internal and external.
- Allowing one person or a discrete group to have sole control of important company information and technology. Dividing authority will go a long way to reduce the risk of the system and the information it holds being invaded from the inside, especially by a disgruntled employee.
- Companies should protect against piracy by setting up an anti-piracy group and demonstrating its commitment to ensuring that its customers receive legitimate, licensed software, and that commercial partners receive the appropriate revenues for the distribution of their software. Further, there should be no hesitation in prosecuting a discovered pirate.
- Be alert to con artists, who approach potential technology users with schemes requiring the payment of advances or up front *seed* money, but then disappearing or never delivering on their end of the contract. Due diligence should be performed before money changes hands.
- Among the risks associated with the operation of purchasing systems are false input of invoices, diversion of payments, and misappropriation of purchases.
- Because high tech involves cutting-edge intellectual property, constant attention should be paid to possible breaches of licensing agreements and patent infringement. The more unique the product, the more it has to be protected.
- Dishonest contractors padding bills on big dollar defense and aerospace contracts are a constant task for government internal auditors.
- Falsified research results at academic and private laboratories.

Not surprisingly, the different fields and/or industries in the high tech sector experience both similar and varying vulnerabilities. Some of the most prevalent are highlighted according to the individual areas within this sector.

Computer Hardware and Software Development, Installation, and Implementation

Most companies or industries concerned about the security of their product focus on attacks from outside. As a result, there are security loopholes for the internal fraudster to slip through. The controls a company establishes are the only way to address and significantly reduce the vulnerabilities of high-tech computer products. These controls should be designed to thwart the outside attack from a hacker, the inside attack by a current or former employee, and the combined attack of an employee and an outsider.

While vandals can attack the machines and hackers can invade the systems, the real problem is with a company's own employees. The days of the giant mainframe housed in a locked, air-conditioned room and operated by only a few people on site are long gone. Today, the proliferation of the personal computer (PC) has permitted the creation of local and wide area networks (LANs and WANs) that give large numbers of people access to the system through workstations both at the home offices and at locations far removed from there. The computer-adept fraudster is now most likely to be a company employee with a good knowledge of the systems and their vulnerabilities.

Disgruntled Employees Can Be a Time Bomb Case Study

U.S. Attorney Robert J. Cleary announced that a federal jury found a former chief computer network administrator guilty of unleashing a computer programming time bomb that deleted all design and production programs of a New Jersey-based high-tech measurement and control instruments manufacturer. The Omega Engineering Corp. of Bridgeport, N.J.—a manufacturing firm serving National Aeronautics and Space Administration (NASA), the Navy, as well as private companies—suffered damages from lost contracts and lost productivity that totaled more than $10 million.

This case illustrates the ironic fact that the tools that allow and facilitate the development of high technology are the very same tools that create the vulnerability and susceptibility of the product. The ability and knowledge of an insider, usually the developer, to adversely use computer software to attack a new product should always be a major concern to any company or industry.

Starting in the early 1990s computer chips were a major commodity in the criminal market. As a result of the high demand and limited supply—chip manufacturers could not produce enough to keep up with the demand—the prices skyrocketed. An underworld trade in high-speed memory chips developed: there were now high-tech thieves. Around the world thieves vandalized the desktop and laptop computers of numerous companies for the sole purpose of stealing these now precious memory chips. The high-tech thefts increased operating costs for businesses. The increased theft-insurance premium for covering company assets was one result. Likewise, consumers were not shielded from this high-tech crime wave.

The central problem of computer hardware and software development is building secure machines and systems. Security is paramount because these machines and systems house a company's intellectual assets, which includes more than secret, technical product information. The computers are the residence of a company's internal operating processes for managing customer lists and analyzing marketing, billing, and every other type of information essential to profitability.

E-Commerce and Cyberfraud

The more employees, customers, and suppliers are connected to the growing number of computers that, in turn, are connected to a company's nationwide or global operations, the more vulnerable a company is to unauthorized intrusions. Probably the scariest aspect of this word-wide hook up is that the intruder does not physically have to invade an entity's premises to do damage. Any place on earth is a good starting point from which to attack a business half way around the world.

Cyberfraud is a crime that is perpetrated, aided, or abetted most often by technology specialists in information systems. The definition covers computer-related crime, theft of proprietary information, electronic intrusion, credit-card fraud, embezzlement, extortion, and sabotage. Businesses use firewalls and encryption, which employ the principle of separation of responsibilities, to compartmentalize the workplace and to protect internal systems from unauthorized external access. However, information and communications systems change rapidly, making security upgrades costly and sometimes difficult to implement. Also, as IT systems get more complex, security becomes even more complicated and layered with slower authorization procedures, which can be time consuming and costly.

E-commerce businesses are faced with the challenge for a market-driven system of controlling costs and increasing profits versus protecting proprietary information. There are an increasing number of cases that illustrate how a fraudster can enrich him- or herself by gaining access to another's intellectual property.

E-Commerce Alias Case Study

In a suit filed in the U.S. District Court for the Eastern District of California, Novell alleged that a Mr. Bonner used several alias accounts on eBay's auction site as a vehicle to distribute unlicensed copies of Novell's Net Services software. Novell contended that Bonner conducted more than forty illegal auctions of its software over a six-month period.

Cases like this one show that not only does the creator of the proprietary property lose but also the intermediary, in this instance the sales channel, which is trying to compete fairly, loses. And the honest customers, who are seeking to acquire legitimate, licensed software, end up confused, harmed, and possibly resolved to stay away from e-commerce.

E-Hacker Havoc Case Study

A recent article in the *Canadian National Post* stated that "[A] Canadian hacker made headlines last autumn when his antics slowed Websites to a crawl. The resulting loss for e-businesses? $1.2 million in revenues. According to an IBM survey, 75% of companies had their sites hacked into at least once last year, and the U.S. Federal Trade Commission reported a $10-billion loss from Internet fraud in 1999."

Another target of a systems invader is the proprietary customer information stored on a company's computers. It is difficult to place a value on this information when it is in the hands of competitors. But there is no doubt that it is worth a lot. The fraudster with the right high-tech knowledge can steal the ideas, customers, and business of another. In the world of e-commerce, the same technology and tools are used to compete legitimately or fraudulently. The sad thing is that the instructions on how to use otherwise legitimate technology is readily available to the potential fraudster on the Internet.

E-Commerce Dirty Dealing Case Study

An Internet bookseller in Boston, MA, which also operated an Internet communications service, was charged in federal court with intercepting electronic communications and the unauthorized possession of password files. The Information presented in court alleged that the purpose of the interception was, in part, to gain a competitive commercial advantage for ALIBRIS/INTERLOC's own online book-selling business by compiling a database of other dealers' purchases and by analyzing the book-selling market. The Information alleged that ALIBRIS's corporate predecessor, INTERLOC, INC. was an on-line bookseller, and also operated a business called Valinet, which provided Internet service in the Greenfield, MA area. INTERLOC provided email service to its customer book dealers. The Information alleged that for periods of time between January and June 1998, ALIBRIS/INTERLOC intercepted email messages sent by online bookseller Amazon.com to ALIBRIS/INTERLOC bookseller clients who had **INTERLOC** email addresses.

Gaining Unauthorized Access Can Lead to Jail Case Study

An Office of the Inspector General (OIG) investigation resulted in the filing of an Information against a contractor's former employee charging him with computer fraud. The Information alleged that the fraudster used his NASA-owned computer workstation to hack into the computers of private businesses. The OIG investigation disclosed that the former employee used his NASA-provided workstation to gain unauthorized access to a computer network domain located at an academic institution. Once he gained access to the domain, he downloaded stored password files. The accused pled guilty to the charge and made restitution to the institution and other business that were victimized.

The high-tech-age ability to warehouse and manipulate data has added a new twist to raiding a competitor's personnel. Because of rapid changes, there is a limited pool of potential employees with the requisite knowledge of the technology, the hardware and expertise. Today's high tech companies have far more to worry about than just protecting their physical and intellectual property. As the expression goes "a company is only as good as its employees . . . ."

One Against Four Case Study

A new competitor, Triple One Technology, started hiring employees away from Four Four Four, Inc., an established IT business. Over a period of time, Triple One wooed Four's CEO and others on down to the level of research analyst. Four's employees were systematically targeted in small groups. Once the pattern of employee raiding was recognized, there was an immediate concern for the loss of intellectual property, which became the stimulus for possible litigation.

When the CEOs of both companies were unable to come to some agreement, Four tightened its security and controls. Employees who left Four were investigated for possible breaches of contract. Their computers and emails were searched for evidence of preparations to take or the actual taking of proprietary information with them to their new jobs. One former employee was caught with proprietary information. He had emailed the proprietary files to himself at home.

It is interesting to note that in this case, although the established business was itself a high-tech company, the information at risk here was the customer lists, pricing sheets, vendor discounts, and structured margins. It is most noteworthy, of course, that all of this information was acquired by hiring away Four's employees who had access to the information. In one underhanded move, Triple One was able to get both the highly trained professional personnel it needed to compete in the global marketplace and to acquire the invaluable inside information that would give it the competitive edge. This particular case was successfully prosecuted under the Industrial Espionage Act.

The advent of e-commerce and the low cost of setting up phony businesses on the World Wide Web make consumers more vulnerable to fraudsters. Names, addresses, credit card numbers and expiration dates are freely sent often without any guarantee that the transmission is protected by one of the available secure line softwares. The Internet enables scam artists to victimize consumers all over the world in simple and inexpensive ways.

An offshore World Wide Web site offering the sale of fictitious goods may attract U.S. consumers who can shop at the site without incurring international phone charges, be contacted through email messages, and may not even know that the merchant they are dealing with is offshore.

The original purpose of the Internet was communication, specifically around the world and between coasts at record speeds. This type of speed can be detrimental when the wrong type of communication is sent, especially because we have not perfected the means to instantly verify the communicated information or its true source.

Cyber-styled Stock Market Manipulation Case Study

Emulex, which is based in Costa Mesa, California, was the target of a stock manipulation scheme. According to the indictment, a false press release was sent to Internet Wire on August 24, 2000, for distribution. The bogus press release, which purportedly was issued by Emulex, claimed that (1) Emulex was under investigation by the SEC, (2) the company's chief executive officer was resigning, and (3) Emulex had revised its latest earnings report to show a loss instead of the profit previously reported.

The false press release was distributed by Internet Wire on the morning of August 25, and a number of news organizations—including CBS Market Watch, Bloomberg, and CNBC—reported the story. As a result of the false press release and its subsequent reportage, the stock price of Emulex plummeted from more than $110 a share to approximately $43 a share in less than one hour. There was also a significant increase in the trading volume of Emulex stock, most of which was done by individual traders—many of whom experienced significant losses because they sold their shares at prices significantly lower than the true value of the stock.

This type of fraudulent Internet activity is easily accomplished with today's technology. The impact of cyberfraud is growing as the number of household computers multiplies and the availability of user-friendly, simpler software makes access to the Internet even easier. Tied to this are the high-tech kids, preteens and teens, who no longer spend time outdoors in physical activity, but rather amuse themselves with new challenges: invading companies worldwide via the Internet.

Kids Will be Kids Case Study

In April 1999, Patrick W. Gregory was responsible for the transmission of a computer program that allowed him to gain unauthorized access to a protected computer owned by "1688.com." Gregory stole banking information and passwords and posted it all on the Internet, and he compromised the site's users' personal email accounts.

Typically, Gregory and his coconspirators would replace the legitimate Web pages of their victims' sites with text and graphics relating to their organization, *globalHell.* In some instances other coconspirators, who were members of *total-kaOs* and *globalHell* would obtain complete and unauthorized control over a victim's system, known as "root level access." Thereafter, *total-kaOs* and *globalHell* members would intentionally crash and delete data on protected computer systems causing untold damage to the victims' networks. The damages were sometimes financial and sometimes intangible, including the loss of faith in the victimized organizations and loss of brand name impact as a result of the public defacements of their web sites.

The Internet provides a con artist with the unprecedented ability to reach millions of potential victims without leaving the comforts of home, wherever in the world that might be. As far back as December 1994 (almost a millennium in computer development time), the Justice Department indicted two people for fraud on the Internet. Among other things, they had placed advertisements on the Internet that promised the potential victims "valuable goods upon payment of money." But the defendants never had access to the goods, and never intended to deliver them to their victims. Both pleaded guilty to wire fraud.

Telecommunications

Telecommunication companies can either be the target of a direct attack or taken over and used by hackers to access targeted companies. Fraudsters can choose to weave their communications through service providers in a number of different countries to hide their tracks. As a result, crimes or abuses that seem to be local in nature might require international assistance and cooperation.

The use of technology and high-tech devices to accomplish the fraudsters' goals is also a key concern of many industries. These devices are used to access either customer information or proprietary company information. These powerful high technologies can have powerful consequences.

Phone Phreak Case Study

By using stolen unauthorized access devices, such as telephone numbers, personal identification numbers (PINs), and credit card numbers, Patrick W. Gregory illegally accessed numerous teleconferences using the facilities of victims AT&T, MCI, Sprint, Latitude Communications, and various other telecommunications providers.

Gregory routinely accessed the teleconferences, which routinely lasted more than six hours, with the aid of unauthorized access devices. This allowed him to steal free telephone service in order to share and coordinate attacks on protected computers throughout the world. Gregory also used the unauthorized access devices to listen to or to disrupt teleconferences of legitimate third parties using the telecommunications services of these victim companies. Specifically, in June 1998, Gregory participated in an AT&T teleconference for which he and others caused billing in excess of $4,200 to be charged to an innocent third party legitimately using the conference services. In October 1998, Gregory, using stolen teleconference access information from Latitude Communications, gained access to Dallas Community College District's teleconference system and caused teleconference classes at the College to be disrupted. That break-in resulted in a telephone charge in excess of $18,500 to be made to the College.

Spam is Junk Food for Computers Case Study

There are also the problems of internal attacks on a company's computer communication systems. A federal grand jury indicted Scott D. Dennis of Anchorage, AK, on April 18, 2000, for allegedly interfering with a government-owned communication system. The indictment states that Dennis, who was the system administrator and computer security officer for the U. S. District Court for the District of Alaska, initiated at least one of five attacks on *Judsys,* which is a mail-list server that runs on a computer owned and operated by the U. S. District Court for the Eastern District of New York.

Dennis attacked the system through an email flood that impaired the availability of the *Judsys* system to others. The system was overwhelmed with *spam,* that is, inappropriate "junk" email. Specifically, *Judsys* subscribed to numerous other mail-list servers on the Internet. When the other mail list servers sent an acknowledging email, *Judsys* was flooded with emails. The *Judsys* computer had to be shut down and taken out of operation, reconfigured, and brought back on-line. An investigation determined that the attacks came from computers traced to Dennis through the Internet Protocol (IP) addresses that were used.

Fraudsters use computers to position themselves in new kinds of consumer fraud that would have never been previously possible. In one case, two hackers in Los Angeles pleaded guilty to computer crimes committed to ensure they would win prizes given away by local radio stations. When the stations announced that they would award prizes to a particular caller, for example, the ninth caller, the hackers manipulated the local telephone switching equipment to ensure that the winning call was their own. Their prizes included two Porsche automobiles and $30,000 in cash. Both of the fraudsters received substantial jail terms.

There are other cases in which the consumer is unknowingly used as a resource for fraudulent telephone calls and other telecommunication scams. According to an FTC complaint, people who visited certain pornographic Web sites were told they had to download a special computer program. Unknown to them, the program secretly rerouted their phone calls from their own local Internet provider to a phone number in Moldova, a former Soviet republic, from which a charge of more than two dollars a minute could be billed. According to the FTC, more than 800,000 minutes of calling time were billed to unsuspecting U.S. customers.

Biotechnology

Biotechnology, a relatively new industry, is at the heart of the development of patents for products derived from the growing knowledge of the human and other genomes. New drugs for humans and animals as well as genetically engineered plants that resist insects, rot and disease are coming from discoveries in this field. The competition for knowledge is intense because of the billions to be earned from sales of these new products. As a result, biotechnology is prone to industrial espionage and to the theft of specialized equipment and computers.

Cloned DNA Does Equal Cloned Patents Case Study

In a recent fraud case involving biotechnology patents, the question was for Promega to prove that it was Cetus' intent to mislead the Patent and Trademark Office through withholding material information in a patent application.

A polymerase chain reaction (PCR) is widely held as one of the most important inventions in molecular biology in the last half of this century. PCR makes it possible to take a small amount of DNA and make many copies of it. Forensic testing, rapid identification of infections, and faster gene manipulation (what once took six months can be done in an afternoon) are all applications of PCR. The key component of PCR is *Taq* polymerase, an enzyme that copies DNA.

In 1992 Hoffman-La Roche sued Promega for breach of license agreement. Maintaining that there were other applications of *Taq* polymerase and that end users were responsible for ensuring that they were licensed to use *Taq* polymerase for PCR, Promega denied the breach of contract claim and countered by challenging the validity of the *Taq* patent. Promega claimed that the Cetus inventors knew that they did not have a novel invention when they applied for the U.S. patent for the use of *Taq* polymerase for PCR and knowingly withheld that information.

The trial court decided in 1996 that it had clear and convincing evidence that Cetus withheld material information from the Patent and Trademark Office in its patent application. Thus, an attempt at fraud through omission failed. Remember, failure to act can be as much a fraudulent act as actually performing a fraudulent act.

Defense and Aerospace

The end of the cold war did not reduce the need to upgrade weapons and equipment for the military. In fact, military and defense needs moved forward with space exploration. Just as in the movies and best-selling books, the development of weapons systems is now and always has been the subject of criminal intent either through espionage or theft. Spies both internal and external are constantly seeking access to secret information. Both military and aerospace contractors often experience cost overruns that sometimes have involved fraudulent overcharging. In general the frauds perpetrated in this area revolve around vendor frauds (both with and without an internal confederate) such as bribery, kickbacks, and false claims.

Conspiracy Where You Least Expect It Case Study

A joint investigation by the OIG, Defense Criminal Investigation Service (DCIS), and Air Force Office of Special Investigations (AFOSI) resulted in an indictment of a NASA contractor's former buyer and the owner of a subcontractor company. The indictment charged them with conspiracy, false claims, and kickbacks.

The investigation disclosed that the former buyer solicited and received kickbacks from the subcontractor totaling $11,000. The subcontractor disguised some of the kickbacks as "ghost" employees. The individuals conspired to inflate invoices billed to the Government through a contract valued at $700,000.

Robotics Contractor's Employee Fraud Case Study

A joint investigation by the OIG, FBI, and DCIS led to an indictment charging three of a contractor's employees with eleven counts of conspiracy to defraud the United States and making false claims on contracts. Two of the three employees were also charged with making false statements to a bank to obtain a line of credit. Criminal Informations were filed against two other employees charging them with conspiracy. At the heart of the fraud were false progress payment requests the employees submitted on which they overstated the contract work performed

False Certification of Microelectronic Devices Case Study

A joint investigation of a NASA/Department of Defense (DOD) contractor by the OIG and the DCIS resulted in an indictment against a contractor and five of its employees for conspiracy, and making false statements and false claims. The indictment alleged that the accused falsely certified that they had performed tests of microelectronic devices in conformance with the Government contract specifications. The fraudulent activity took place over a nine-year period. The devices had application in a number of significant NASA and military programs, including the Space Shuttle, F-14 aircraft, and submarines.

A separate indictment alleged that a Government quality assurance representative falsely certified that he had witnessed the tests at the contractor site (the internal cooperative fraudster).

High-Tech Crime Caught by Low-Tech Method Case Study

Fraud perpetrated through old-fashioned, low-tech methods, in this case mail fraud, can show up in high-tech situations. For example, an investigation by the OIG, FBI, DCIS, Department of Transportation (DOT), and AFOSI led to the indictment of a fastener supplier and its owner. The indictment on fifteen counts of mail fraud charged them with selling commercial grade fasteners to the Government, but falsely certifying they met more stringent military specifications. The fasteners were used on Space Shuttle applications, other NASA spacecraft, FAA radar systems, and DOD radar and launch systems.

Trade Secrets Theft Case Study

An OIG investigation resulted in charges against two of a contractor's former employees at a NASA Center in connection with the theft of trade secrets. The investigation confirmed that one of the former employees offered to sell what was purported to be technical and cost proprietary data relating to a NASA procurement competition. A defendant agreed to sell computer disks containing confidential material for $25,000. He claimed that the information pertained to a pending NASA procurement program valued at approximately $30 million.

The DOD has 2.1 million computers on 10,000 LANs around the world and requires a high level of proprietary encryption to protect itself. Without the encryption facility, the whole DOD system would be open to compromise because it runs over public circuits using commercial software and hardware. The threat to the DOD system is mainly from international terrorists, criminals, or those wishing to spread knowledge of weapons of mass destruction. The DOD has allocated more than $500 million to develop a secure system. One of the most important aspects of the new system has been controls on the export of encryption technology.

Other Leading Edge Scientific or Industrial Research and Development

Academic research as well as research in private labs at major manufacturers are also the targets of theft and industrial espionage. Academic research presents a special case because so much of it is done with publicly funded resources. The publication in academic journals of falsified university-based and funded research to advance the careers of the researchers is not unheard of.

In the private sector, research results are kept under wraps as much as possible because of the huge amounts of money to be made from the development and marketing of products designed with the proprietary information. Because many companies may be simultaneously, but independently, carrying on similar research, the resulting patents, trademarks, and copyrighted materials are frequently the subject of litigation. It is a question of who won the race, and was it won legitimately or through fraud. The latter reflects the loser's mentality: we could only have lost if our competition cheated.

4.3 Key Preventative Controls

Internal controls are the most frequently cited method for reducing the risk of fraud and detecting fraud. Encouraging employees to take an active role in reducing fraud also pays dividends. Sometimes, fraud is discovered by accident. A survey, by Ernst & Young (*Fraud, the Unmanaged Risk : An International Survey of the Effects of Fraud on Business*, May 1996), suggested that as much as 60 percent of reported frauds, ". . . were discovered by chance, i.e., by outside information, anonymous external tip-off, internal whistle-blower, accident or change of management."

Tip-offs from internal or external sources are an important source of fraud detection. Many businesses have installed 'hotlines' or 'helplines' to enable staff and outsiders to voice their concerns about behavior that may indicate the presence of fraud. These lines may be manned or unmanned (that is, linked to an answering machine). The advantage of a manned line is that it provides a live contact from whom the whistle-blowing staff member can seek advice on fraud risks, the internal controls, and how to proceed.

Make sure you know your employees. Verifying backgrounds, references, and past employment history is key to a company's reducing internal exposure to fraud. This is especially true for high tech departments in which easy access to important, proprietary information is part of the normal work activities. Employees are not always who they appear to be. Recent studies suggest that many dotcom executives have suspicious, if not totally suspect, backgrounds.

Some environments are generally more vulnerable to fraud. Consider the following, for example:

- Management does not perceive fraud to be a risk or management has made no effort to assess its fraud risk exposure
- Management ignores irregularities; takes the ostrich "head-in-the-sand" approach
- Management has failed to clearly communicate to its staff the types of behavior that are not acceptable
- For one reason or another, management has failed to keep staff morale at an acceptably high level
- Management's actions have induced high staff turnover
- Management failed to provide adequate staff training for the systems and procedures its personnel operates

Fraudsters frequently use a number of techniques to conceal evidence of their crimes. There are, however, certain signs that generally indicate the presence of fraud. For example, consider the following telltale signs.

- Staff who take no holidays or who regularly work alone after normal hours or on weekends
- Employees whose lifestyles appear to exceed their salaries
- Staff who won't delegate certain tasks, keep their work to themselves, and discourage others from learning about their jobs' responsibilities
- Staff who resent being questioned about their work or who answer evasively when questioned about their work
- Staff who always have plausible excuses—always a little too smooth—for errors
- Staff who insist on dealing personally with certain suppliers or particular transactions

This is not an exhaustive list but a reminder that line managers should be alert to behavior that, in isolation or in conjunction with other possible warning signs, may suggest the concealment of irregular activities.

Many organizations use the format of a fraud policy statement to communicate the organization's attitude and approach to the threat of fraud. These statements may include some or all of the following points.

- Assigning responsibilities for the overall management of fraud; that is, establishing the necessary controls, monitoring the operation of the controls, and handling the discovered fraud
- The formal procedures that staff should follow when a fraud is discovered
- Providing the necessary staff training for reducing the opportunities for fraud and increasing the possibility of detecting fraud
- Creating of awareness among the staff that response plans exist, and will be implemented, to deal with and minimize the damage caused by any fraudulent attack

Organizing the fraud reduction and discovery teams involves assigning responsibility to individuals or groups so that they work together as a team to achieve the desired objectives in the most efficient manner. Major principles in establishing the organizational structure to combat fraud are:

- Clearly defining the responsibilities of individuals for resources, activities, objectives, and targets. For example, establishing levels of authority as a preventive measure, such as setting dollar limits on the payments that can be authorized by an individual without a second signature. To be effective, periodic audits should be made to ensure that transactions have been properly authorized
- Establishing clear reporting lines that embody the most effective chain of command to allow adequate supervision
- Separating duties to reduce opportunities for fraud. This is also largely a preventive measure that ensures that all the key functions and controls over a process are not carried out by the same individual; for example, purchasing goods should be kept separate from the receiving function; similarly the acknowledgement of the receipt of goods should be separated from the authority to pay invoices
- And, as a general rule, avoiding placing too many functions in any one individual's hands, regardless of how responsible that employee may appear to be

Suggested Controls for Contract Frauds in the Aerospace and Defense Industries

The following will help to ensure that proper contract tendering procedures will not fail because of collusion or cozy relationships between staff and contractors.

- An approved list of suppliers should be considered. This list should be regularly updated with any amendments appropriately authorized.
- Clear and unambiguous tendering procedures should be established. Adherence to these procedures should be closely monitored.
- The bidders should deliver tenders directly to those responsible for selection without passing through intervening hands not involved in the bidding process.
- Late tenders should not be accepted.
- Staff should be required to declare any personal interests or possible conflict of interests they may have that could affect the tendering process.

The following will help to assure that payments are only made for work actually performed.

- To prevent collusion between a contractor and an employee, invoices should only be paid when accompanied by an independent certification that the contracted work has been satisfactorily completed.
- The purchaser of services should maintain a register of contracts in progress.
- The only contracts that can be added to the contract register must be properly approved and authorized according to established protocols.
- All contract changes in the original contract terms should be documented, change orders should be sequentially numbered, with the documentation prepared in an agreed format and authorized before payment.

- Prior to approval of a payment, the payment should be reconciled with the budget by someone other than the person requesting the payment be made. Further, the payment should be within the parameters of the planned expenditures.

Suggested Controls for Computer Hardware and Other Valuable Assets

The following describes some of the controls that should be in place to reduce the threat of fraud or other irregularities associated with a company's procurement and proper use of computer hardware and other valuable assets within departments.

- An up-to-date asset register should be maintained with the assets assigned to individual budget centers.
- The assets should be adequately described and identified on the asset register.
- When possible, the assets should be marked for identification.
- Controls should be established to assure the physical security of the assets.
- Spot checks should be regularly carried out to ensure the existence of the listed assets where they are supposed to be.
- Details of proposed sales, reason for the sales, expected prices to be received, the date of the sales, and expected results should be reviewed and approved prior to the sales. There should be a follow-up after the sale to review the results including confirming that the expected price was in fact received and that the funds received were promptly deposited in the appropriate account.

Risks Associated with Sensitive Documentation

The following describes some of the controls that should be in place to reduce the threat of fraud or other irregularities that could arise from improper access to sensitive information or misuse of information for private gain.

- Controls should be established to protect third party's information held on company computers, and steps should be taken to assure compliance with the requirements of the Data Protection Act; further, staff should be informed of the rules.
- Official documentation should be held in a secure environment.
- Vetting of staff should be at an appropriate level, which should relate to the nature of the post held.
- Access to computer records should be entered into a log and spot checks should be made to confirm that there were independently verified valid reasons for any unusual accesses.

4.4 Checklist and Grids

A fraud risk management checklist specific to the high-technology sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

(Text continued on page 23)

High Technology Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the high technology sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Inventory fraud such as theft or diversion of computer chips (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Management fraud, such as false financial statements, inflating income, manipulating share prices, insider trading, and the like, (related controls include good corporate policies [especially strong enforcement], and strong internal audit function)	☐	☐	☐	___
• Sabotage and espionage by employees, competitors, or others (related controls include physical access restrictions, and good corporate policies particularly at the hiring stage)	☐	☐	☐	___
• Outsider frauds such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___
• Commercial crime by or against the organization, including patent infringement, antitrust violations, and organizational bribe giving (related controls include good corporate policies [especially strict enforcement and supervision], strong internal audit functions, and periodic outside audits)	☐	☐	☐	___
b. Have the following vulnerability areas for the high technology sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds, such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___

(continued)

HIGH TECHNOLOGY SECTOR CHECKLIST *(continued)*

High Technology Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, strong internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Secret commissions, kickbacks, etc. (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___

Fraud Vulnerability Grid High Technology Sector	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (for example, front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers, or credits)		X	
Inventory fraud (theft or diversion of computer chips)	X		
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like			X
Manipulation of financial statements by officers	X		
Manipulation of share prices by directors and officers	X		
Employee sabotage or espionage	X		
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (for example, inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)	X		
Con schemes or extortion by outsiders	X		
Copyright piracy, patent infringement, and the like	X		
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)		X	
Environmental crime (for example, dumping)		X	
False advertising		X	
Insider trading and antitrust violations	X		
Money laundering		X	
Organizational bribe giving	X		
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy		X	

(continued)

FRAUD VULNERABILITY GRID—HIGH TECHNOLOGY SECTOR *(continued)*

Fraud Vulnerability Grid High Technology Sector	High	Avg	Low or NA
Corporate Policies:			
Corporate mission statement and code of ethics	X		
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	
Fair performance appraisal and review system		X	
Employee screening and testing before hiring	X		
Management acting as a good role model	X		
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like		X	
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both		X	
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)	X		
Regular off-site backups of programs and data files	X		
Software controls (for example, antivirus, full documentation)	X		
Programmer controls (for example, supervision, antisabotage)	X		
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud	X		
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (for example, exceptions, customer complaints)		X	
Auditors (internal, external)		X	
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft.)		X	

5 MANUFACTURING

5.1 Introduction

The manufacturing sector contains numerous varieties of businesses. A few of the major segments include:

- Auto and auto parts manufacturing
- Clothing and textile industries
- Production of other consumer goods (ranging from durable goods, such as televisions, washing machines, and furniture to everyday items such as soap and garbage bags)
- Food processing and packaging

This sector is fairly average in its overall susceptibility to fraud.

5.2 Key Vulnerabilities

Some of the key vulnerabilities to fraud in this sector include:

- Employee frauds, typically involving inventory, accounts payable, or payroll. These frauds are sometimes carried out in collusion with outsiders.
- Supplier frauds such as overbilling or materials substitution.
- Some forms of commercial crime, such as environmental crime, or violation of occupational health and safety (OSHA) laws, or both.

5.3 Key Preventive Controls

The manufacturing sector is fairly average across the board in terms of the importance of specific controls.

The best defense against the potential for inventory, accounts payable, and payroll frauds is a good segregation of duties and regular accounting reconciliations. Included in the latter should be periodic inventory counts for comparison with the perpetual records. Consistent unexplained shortages in raw materials, for example, may indicate the presence of fraud.

5.4 Checklist and Grids

A fraud risk management checklist specific to the manufacturing sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Manufacturing Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the manufacturing sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Inventory fraud such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, periodic external audits [especially confirmations], and supervision)	☐	☐	☐	___
• Outsider frauds such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___
• Commercial crime by the organization, including environmental crime and violating occupational health and safety (OSHA) laws (related controls include good corporate policies [especially strict enforcement], supervision, and strong internal audit functions)	☐	☐	☐	___
b. Have the following vulnerability areas for the manufacturing sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds such as cash theft, cash skimming or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions, [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___

MANUFACTURING SECTOR CHECKLIST *(continued)*

Manufacturing Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Management fraud, such as false financial statements, inflating income, manipulating share prices, insider trading, etc. (related controls include good corporate policies [especially strong enforcement, and strong internal audit functions])	☐	☐	☐	___
• Sabotage and espionage by employees, competitors or others (related controls include physical access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___

Fraud Vulnerability Grid **Manufacturing Sector**	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers or credits)		X	
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)	X		
Payroll frauds (for example, ghost employees)	X		
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like		X	
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers		X	
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)	X		
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like		X	
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)		X	
Environmental crime (for example, dumping)	X		
False advertising			X
Insider trading		X	
Money laundering		X	
Organizational bribe giving			X
Tax evasion		X	
Violating occupational health and safety (OSHA) laws	X		
Violation of privacy			X
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)		X	
Employee relations (for example, fair compensation, counseling)		X	

Fraud Vulnerability Grid—Manufacturing Sector *(continued)*

Fraud Vulnerability Grid Manufacturing Sector	High	Avg	Low or NA
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)		X	
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable, and inventory)	X		
Customer account statements, or confirmations, or both		X	
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)		X	
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

6 MEDIA AND COMMUNICATIONS

6.1 Introduction

The media and communications sector includes:

- Book publishing
- Print and broadcast media
- Music and motion picture industries
- Telephone, cable, and satellite industries

Although certain parts of this sector are in decline (for example, newspaper and fiction-book publishing), for the most part the sector has been characterized by very high growth, especially over the last two decades. As is the case with the high technology sector, the growth and the glamorous nature of some parts of the media and communications sector contribute to the risk of fraud.

6.2 Key Vulnerabilities

Some of the key vulnerabilities to fraud in this sector include:

- Frauds by officers or directors, such as fraudulent financial reporting, manipulation of share prices, insider trading, and antitrust violations.
- Frauds by customers. Some parts of this sector–for example, telephone and cable companies–are vulnerable to equipment theft by customers.
- Con artists, who may approach this sector with schemes requiring the payment of advances or up front *seed* money, but then disappear or never deliver on their end of the contract.
- Copyright and patent infringement, which can be a problem for some parts of this sector–for example, unauthorized decoder boxes in the cable industry.
- Violation of privacy. The nature of the sector can sometimes make this a problem, although violations have to be weighed against other rights, such as freedom of the press.

6.3 Key Preventive Controls

Some of the key fraud prevention controls in the media and communications sector include:

- A strong code of ethics with strict sanctions for any breach.
- Strong enforcement–for example, ensuring that managers and officers are severely dealt with for any antitrust violations (by both the company and society generally), and prosecuting copyright and patent infringers to the fullest extent of the law.
- Physical access controls, such as credit screening of customers before allowing them to walk off with leased company equipment.
- Good computer security, to protect against fraud and avoid breaches of confidentiality, or the misuse of information, or both.

- A strong internal audit function and periodic external audits. This should include periodic direct confirmation of customer statement information.

6.4 Checklist and Grids

A fraud risk management checklist specific to the media and communications sector follows along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Media and Communications Sector Checklist	**Yes**	**No**	**NA**	**Ref**
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the media and communications sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Management fraud, such as making false financial statements, inflating income, manipulating share prices, insider trading, and the like (controls include good corporate policies such as strong enforcement, and internal audit functions)	☐	☐	☐	___
• Customer and outsider frauds, such as theft of equipment, copyright and patent infringement, con schemes, (related controls include good corporate policies, supervision, and enforcement)	☐	☐	☐	___
• Commercial crime by the organization, including violation of privacy (related controls include good corporate policies [especially strict enforcement and supervision])	☐	☐	☐	___
b. Have the following vulnerability areas for the media and communications sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Computer crime (related controls include job descriptions, division of duties, annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___
• Front-end and lapping frauds such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___

(continued)

MEDIA AND COMMUNICATIONS SECTOR CHECKLIST *(continued)*

Media and Communications Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Inventory fraud such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Sabotage and espionage by employees, competitors or others (related controls include physical access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___

Fraud Vulnerability Grid **Media and Communications Sector**	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers or credits)		X	
Inventory fraud (for example, theft, diversion)		X	
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like			X
Manipulation of financial statements by officers	X		
Manipulation of share prices by directors and officers	X		
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like	X		
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders	X		
Copyright piracy, patent infringement, and the like	X		
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)		X	
Environmental crime (for example, dumping)		X	
False advertising		X	
Insider trading and antitrust violations	X		
Money laundering		X	
Organizational bribe giving			X
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy	X		
Corporate Policies:			
Corporate mission statement and code of ethics	X		
Enforcement (for example, dismissal and prosecution for fraud)	X		

(continued)

FRAUD VULNERABILITY GRID—MEDIA AND COMMUNICATIONS SECTOR *(continued)*

Fraud Vulnerability Grid Media and Communications Sector	High	Avg	Low or NA
Employee relations (fair compensation, counseling, and the like)		X	
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (locks, alarms, security), and the like	X		
Job descriptions, segregation-duplication of duties, and the like		X	
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both	X		
No management override of controls		X	
Computer Controls:			
Access restrictions (physical access, passwords, and the like)	X		
Regular off-site backups of programs and data files	X		
Software controls (antivirus, full documentation, and the like)	X		
Programmer controls (supervision, antisabotage, and the like)	X		
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (fidelity, fire, liability, theft, and the like)		X	

7 Nonprofit

7.1 Introduction

The nonprofit sector, for purposes of this section, consists primarily of charitable and benevolent organizations. It excludes operations set out under the government sector heading in section 3.

Except for cash theft and skimming, this sector is generally less prone to fraud from either within or outside the organization. However, there are a number of commercial crime risks.

7.2 Key Vulnerabilities

The key vulnerabilities to fraud in this sector include:

- Employee or volunteer frauds, typically involving the theft or skimming of cash.
- Commercial crime involving such things as breach of trust (that is, cash theft or skimming at the organizational level), con schemes in which funds received are not used for the advertised purposes, and tax evasion by phony charities. Since this sector collects large volumes of information in the form of mailing lists and other data about contributors, there is also the potential for abuse of this information, invasion of privacy, and so on.

7.3 Key Preventive Controls

Three key fraud prevention controls in the nonprofit sector are:

1. Strong enforcement, that is ensuring that employees are severely dealt with for any breach of the law. This is important to send a deterrent message as well as to maintain public faith and support in the organization.
2. Job descriptions that are clear and adhered to, especially with respect to segregation and duplication of duties. For example, the opening of mail should be carefully controlled because it may contain cash. An appropriate system might be for two people to open mail, one of whom records cash receipts in a log for later balancing against deposit slips, charitable receipts issued, and so on.
3. Follow-up of contributor complaints (for example, no receipt received).

7.4 Checklist and Grids

A fraud risk management checklist specific to the nonprofit sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Nonprofit Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the nonprofit sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Commercial crime by the organization, including breach of trust, false advertising, tax evasion, and violation of privacy (related controls include good corporate policies [especially strict enforcement and supervision], and strong internal audit functions)	☐	☐	☐	___
b. Have the following vulnerability areas for the nonprofit sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, internal and external audit [especially confirmations], and supervision)	☐	☐	☐	___
• Outsider frauds such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___

Fraud Vulnerability Grid Nonprofit Sector	High	Avg	Low or NA
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)	X		
Accounts receivable (lapping, phony customers or credits, and the like)		X	
Inventory fraud (for example, theft, diversion)		X	
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like			X
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers			X
Employee sabotage or espionage			X
External Frauds:			
Customer theft, false instruments or claims, and the like			X
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)			X
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and so on			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)	X		
Environmental crime (for example, dumping)		X	
False advertising (perpetration of con schemes)	X		
Insider trading			X
Money laundering		X	
Organizational bribe giving		X	
Tax evasion (illegitimate charities)	X		
Violating occupational health and (OSHA) safety laws		X	
Violation of privacy	X		
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		

(continued)

FRAUD VULNERABILITY GRID—NONPROFIT SECTOR *(continued)*

Fraud Vulnerability Grid Nonprofit Sector	High	Avg	Low or NA
Employee relations (for example, fair compensation, counseling)		X	
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)		X	
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations			X
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both		X	
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, contributor complaints)	X		
Auditors (internal, external)		X	
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

8 Professional Services

8.1 Introduction

The professional services sector includes:

- Accountants
- Architects and engineers
- Doctors, dentists, and other medical professionals
- Lawyers

The distinguishing characteristics of this sector are: (1) the form of the business–partnership, profesional corporation, limited liability company or–sole practitioner; and (2) the professional-client relationship, as well as an element of public trust.

Because the management of the business is also generally in the hands of the ownership, there is more at stake here in terms of fraud losses. Every dollar lost to fraud is a dollar out of the professional's pocket, and not merely a management embarrassment.

8.2 Key Vulnerabilities

Some of the key vulnerabilities to fraud in this sector include:

- Frauds involving accounts receivable, for example, accounts receivable lapping schemes. Also, in partnership situations, some partners may commit fraud by undertaking work directly, or billing clients directly, or both, rather than for the benefit of the partnership as required in the partnership agreement.
- Inflated expense reports.
- Breach of trust such as theft of client funds.

8.3 Key Preventive Controls

Some of the key fraud prevention controls in the professional services sector include:

- A strong code of ethics.
- Good basic controls such as (1) job descriptions, such as appropriate segregation of duties, (2) mandatory annual vacations, (3) regular accounting reconciliations, and (4) no management override of basic controls.
- Good computer controls especially in the area of access restrictions and disaster recovery contingencies. This is important not only to ensure smooth operations, but also to avoid breaches of confidentiality, or the misuse of information, or both.
- An awareness of the possibility of fraud, something that is absent among many nonaccounting professionals. Doctors and lawyers, for example, are often unaware of the issue because they are too preoccupied with the practice of their own profession.

Adequate insurance is also important, but more from a liability standpoint than in the areas of theft or fidelity.

8.4 Checklist and Grids

A fraud risk management checklist specific to the professional services sector follows along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Professional Services Sector Checklist	**Yes**	**No**	**NA**	**Ref**
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the professional services sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to patient or client complaints or confirmation discrepancies], and good management policies [especially strict enforcement])	☐	☐	☐	___
• Inflated expense report fraud (related controls include internal audit and supervision)	☐	☐	☐	___
• Commercial crime by the organization, including breach of trust and money laundering (related controls include good management policies [especially strict enforcement and supervision], and strong internal audit function and periodic external audits	☐	☐	☐	___
b. Have the following vulnerability areas for the professional services sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Sabotage and espionage by employees, competitors, or others (related controls include physical access restrictions, and good management policies [particularly at the hiring stage])	☐	☐	☐	___
• Outsider frauds, such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good management policies and supervision)	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___

Fraud Vulnerability Grid Professional Services Sector	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, personal billings)	X		
Inventory fraud (for example, theft, diversion)			X
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)			X
Inflated expense reports by managers and others	X		
Bid rigging, kickbacks, secret commissions, and so on			X
Manipulation of financial statements by the owning professionals			X
Manipulation of valuation of ownership interest by the owning professionals			X
Employee sabotage or espionage		X	
External Frauds:			
Client or patient theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like		X	
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)	X		
Environmental crime (for example, dumping)			X
False advertising		X	
Money laundering		X	
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy		X	
Professional Policies:			
Mission statement and code of ethics	X		
Enforcement (for example, dismissal and prosecution for fraud)		X	
Employee relations (for example, fair compensation, counseling)		X	
Fair performance appraisal and review system		X	

FRAUD VULNERABILITY GRID—PROFESSIONAL SERVICES SECTOR *(continued)*

Fraud Vulnerability Grid Professional Services Sector	High	Avg	Low or NA
Employee screening and testing before hiring		X	
Senior professionals acting as a good role models		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)		X	
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations	X		
Accounting reconciliations (bank, accounts receivable, accounts payable variance)	X		
Patient or client account statements, or confirmations, or both		X	
No management override of controls	X		
Computer Controls:			
Access restrictions (for example, physical access, passwords)	X		
Regular off-site backups of programs and data files	X		
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Professionals' awareness of fraud or possibility of fraud	X		
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Senior professional's follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)		X	
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)	X		

9 Real Estate

9.1 Introduction

For purposes of this section, the real estate sector includes principals or agents conducting the following kinds of operations:

- Buying and selling of commercial and residential real estate (land and buildings)
- Leasing or rental of commercial and residential real estate (land and buildings)

9.2 Key Vulnerabilities

Three key vulnerabilities to fraud in this sector include:

1. Employee frauds involving cash, accounts receivable, or the acceptance of secret commissions.
2. Con schemes involving inflated real estate values, for example flipping a property several times in nonarm's-length transactions–each time increasing the price–in order to ultimately induce an arm's-length third-party to pay a fraudulently inflated price. A variation of this is when the fraudulently inflated price is used to obtain an inflated mortgage or loan on the property.
3. False advertising or representation concerning the property being sold, leased, or rented.

9.3 Key Preventive Controls

This sector is quite average in terms of the importance of specific controls.

Some of the best defenses against fraud in this sector include:

- Strong enforcement, (for example, ensuring that managers and officers are severely dealt with for any violations of law or the company's policies).
- Adequate segregation of duties (for example, between cash handling and record keeping).
- Good supervisory and audit-investigative controls (for example independent checks to ensure that purported real estate values make sense).

9.4 Checklist and Grids

A fraud risk management checklist specific to the real estate sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Real Estate Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the real estate sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds, such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Outsider frauds, such as con schemes (related controls include good corporate policies and supervision)	☐	☐	☐	___
• False advertising and representation, (related controls include good corporate policies [especially strict enforcement and supervision], and strong internal audit functions and periodic external audits	☐	☐	☐	___
b. Have the following vulnerability areas for the real estate sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Management fraud, such as false financial statements, inflating income, and the like (related controls include good corporate policies [especially strong enforcement], and strong internal audit functions)	☐	☐	☐	___

REAL ESTATE SECTOR CHECKLIST *(continued)*

Real Estate Sector Checklist	Yes	No	NA	Ref
• Sabotage and espionage by employees, competitors or others (related controls include physical access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___
• Commercial crime by the organization, including breach of trust, environmental crime, money laundering, tax evasion, and violating occupational health and safety (OSHA) laws (related controls include good corporate policies [especially strict enforcement and supervision], and strong internal audit functions	☐	☐	☐	___

Fraud Vulnerability Grid Real Estate Sector	High	Avg	Low or NA
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)	X		
Accounts receivable (for example, lapping, phony customers or credits)	X		
Inventory fraud (for example, theft, diversion)			X
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions and the like	X		
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers		X	
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders	X		
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)		X	
Environmental crime (for example, dumping)		X	
False advertising or representation	X		
Insider trading		X	
Money laundering		X	
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy			X
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	

FRAUD VULNERABILITY GRID—REAL ESTATE SECTOR *(continued)*

Fraud Vulnerability Grid Real Estate Sector	High	Avg	Low or NA
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)		X	
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)		X	
Customer account statements, or confirmations, or both		X	
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud	X		
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both	X		
Supervisor follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)	X		
Forensic accountants and investigators	X		
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

10 Recreation

10.1 Introduction

The recreation sector includes operations such as:

- Amusement parks
- Movie theaters
- Professional sports clubs
- Golf, tennis, and similar sport or recreation clubs

10.2 Key Vulnerabilities

With one major exception, this sector actually has a relatively low vulnerability to fraud. Unfortunately, the exception involves a very important asset: cash. However, controls over cash tend to be well developed in most of these businesses, so that in practice the main risk is outright theft of cash rather than fraud.

Because of the seasonal and part-time nature of much of the employment in this sector, the opportunity for payroll-related fraud may also be slightly higher.

10.3 Key Preventive Controls

The key fraud prevention control in this sector is good cash control. This includes good physical controls (for example, cash register-ticket dispensing systems with accompanying counters, all of which provide an audit trail), segregation of duties for cash handling and record-keeping, and accounting reconciliations.

Other important controls are: (1) a termination-prosecution policy for the commission of fraud or theft, and (2) a good internal audit function.

10.4 Checklist and Grids

A fraud risk management checklist specific to the recreation sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Recreation Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the recreation sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds, such as cash theft and cash skimming (related controls include admission counters, physical controls and surveillance, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Payroll fraud [for example, ghost employees], (related controls include strong internal audit and supervision)	☐	☐	☐	___
b. Have the following vulnerability areas for the recreation sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable fraud, such as phony suppliers (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Sabotage and espionage by employees, competitors or others (related controls include physical access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___
• Outsider frauds such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___
• Commercial crime by the organization, including environmental crime, false advertising, money laundering, tax evasion, violating occupational health and safety (OSHA) laws, and violation of privacy (related controls include good corporate policies [especially strict enforcement and supervision], and strong internal audit function and periodic external audits	☐	☐	☐	___

Fraud Vulnerability Grid **Recreation Sector**	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)	X		
Accounts receivable (for example, lapping, phony customers or credits)			X
Inventory fraud (for example, theft, diversion)			X
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)	X		
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like			X
Manipulation of financial statements by officers			X
Manipulation of share prices by directors and officers			X
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like		X	
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)			X
Environmental crime (for example, dumping)		X	
False advertising		X	
Insider trading			X
Money laundering		X	
Organizational bribe giving			X
Tax evasion		X	
Violating occupational health and safety (OSHA) laws			X
Violation of privacy		X	
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		

(continued)

FRAUD VULNERABILITY GRID—RECREATION SECTOR *(continued)*

Fraud Vulnerability Grid Recreation Sector	High	Avg	Low or NA
Employee relations (for example, fair compensation, counseling)		X	
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)	X		
Customer account statements, or confirmations, or both			X
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

11 Natural Resources

11.1 Introduction

For purposes of this section the natural resource sector primarily includes entities conducting mining, and oil and gas operations.

11.2 Key Vulnerabilities

Some of the key vulnerabilities to fraud in this sector are:

- Inventory, accounts payable, payroll, and expense report frauds. Because of the large-project nature of the resource sector, companies can be particularly vulnerable to these types of frauds.
- Frauds–by senior managers, officers, or directors–such as bid rigging, kickbacks, or secret commissions; fraudulent financial reporting, stock touting and manipulation of share prices; insider trading and antitrust violations; or organizational bribe giving as part of the contract bidding process. Just as in the high technology sector, many stock-related frauds involve mining companies.
- Supplier frauds involving inflated prices, product substitution, or substandard materials.
- Commercial crime in the areas of environmental crime and the violation of occupational health and safety (OSHA) laws.

11.3 Key Preventive Controls

Some of the more important controls in the resource sector include:

- A strong code of ethics with strict sanctions for any breach.
- Strong physical controls, particularly with respect to the company's precious inventory.
- Supervisor awareness of fraud and the possibility of fraud.
- A strong internal audit function, and periodic external audits.

11.4 Checklist and Grids

A fraud risk management checklist specific to the natural resources sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Natural Resources Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the natural resources sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Inventory fraud, such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Management fraud, such as false financial statements, inflating income, manipulating share prices, insider trading, and the like (related controls include good corporate policies [especially strong enforcement], and strong internal audit functions and periodic external audits)	☐	☐	☐	___
• Sabotage and espionage by employees, competitors, or others (related controls include physical access restrictions, and good corporate policies particularly at the hiring stage)	☐	☐	☐	___
• Outsider frauds, such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___
• Environmental crime, and violating occupational health and safety (OSHA) laws (related controls include good corporate policies [especially strict enforcement and supervision], and strong internal audit functions)	☐	☐	☐	___

NATURAL RESOURCES SECTOR CHECKLIST *(continued)*

Natural Resources Sector Checklist	**Yes**	**No**	**NA**	**Ref**
b. Have the following vulnerability areas for the natural resources sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and accounts receivable lapping frauds (related controls include job descriptions, division of duties, annual vacations, regular accounting reconciliations, follow-up of exceptions, [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Computer crime (related controls include job descriptions, division of duties, annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___

Fraud Vulnerability Grid Natural Resources Sector	High	Avg	Low or NA
Internal Frauds:			
Cash theft, skimming or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers or credits)		X	
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)	X		
Payroll frauds (for example, ghost employees)	X		
Inflated expense reports by managers and others	X		
Bid rigging, kickbacks, secret commissions, and the like	X		
Manipulation of financial statements by officers	X		
Manipulation of share prices by directors and officers	X		
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)	X		
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like		X	
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)			X
Environmental crime (for example, dumping)	X		
False advertising		X	
Insider trading	X		
Money laundering		X	
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety (OSHA) laws	X		
Violation of privacy			X
Corporate Policies:			
Corporate mission statement and code of ethics	X		
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	

FRAUD VULNERABILITY GRID—NATURAL RESOURCES SECTOR *(continued)*

Fraud Vulnerability Grid Natural Resources Sector	High	Avg	Low or NA
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like		X	
Mandatory annual vacations		X	
Accounting reconciliations (especially inventory)	X		
Customer account statements, or confirmations, or both		X	
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud	X		
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)		X	
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

12 RETAIL

12.1 Introduction

The retail sector is one of the largest and its diversity precludes a comprehensive list of its elements. Any operation that caters to the consumer, from department stores to specialty retail stores (clothing, hardware, and so on), fits this category.

Outright theft rather than fraud is the key threat to the retail sector. Just as the insurance sector is very conscious of the cost of fraud to its industry, the retail sector is very conscious of the cost of theft. Both industries regularly research and publish estimates of the extent of fraud and theft in their industries, which is substantial.

12.2 Key Vulnerabilities

As noted, the key vulnerability in this sector stems not so much from fraud as it does from theft by the industry's employees and its customers, perhaps in equal measure although shoplifting by customers receives by far the greatest amount of publicity.

Major fraud risks can involve cash, accounts receivable, and inventory, because all of these are important to the industry. Outright theft of cash and especially inventory–by both customers and employees–receives the largest amount of attention, and it is undeniably the biggest in terms of losses. However, the fraud risks in other areas should not be ignored.

The heavily computerized nature of the industry, even among smaller retailers, means that the opportunity to use computers in fraud is also increased.

On the commercial crime side, false advertising is a major problem in the industry, even among some large retailers who have been charged and convicted of it. Tax evasion can also be a problem, but mainly among smaller retailers who make cash-only deals to avoid sales and excise taxes.

12.3 Key Preventive Controls

Among retailers of any significant size–for *Mom and Pop* stores, see section 13, Small Business–virtually all the basic and computer controls are critical. Obviously, good physical security–especially control over cash and inventory–are the most important. These controls range from good point of sale and cash register systems that provide a proper audit trail, to security surveillance systems that dissuade thieves.

Other important controls are: (1) a termination-prosecution policy for the commission of fraud or theft, (2) supervisory follow-up on all customer complaints, and (3) a good internal audit function.

12.4 Checklist and Grids

A fraud risk management checklist specific to the retail sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Retail Sector Checklist	**Yes**	**No**	**NA**	**Ref**
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the retail sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds, such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies especially strict enforcement)	☐	☐	☐	___
• Inventory fraud, such as customer or employee theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___
• False advertising and tax evasion (related controls include good corporate policies, strict enforcement, and internal audit functions)	☐	☐	☐	___
b. Have the following vulnerability areas for the retail sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___

RETAIL SECTOR CHECKLIST *(continued)*

Retail Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Management fraud, such as false financial statements, inflating income, and the like (related controls include good corporate policies [especially strong enforcement], and strong internal audit functions and periodic external audits)	☐	☐	☐	___
• Sabotage and espionage by employees, competitors or others (related controls include physical access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___
• Outsider frauds, such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___

Fraud Vulnerability Grid Retail Sector	High	Avg	Low or NA
Internal Frauds:			
Cash theft, skimming or lapping (front-end frauds)	X		
Accounts receivable (for example, lapping, phony customers or credits)	X		
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions (to buyers)		X	
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers			X
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like	X		
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud	X		
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)			X
Environmental crime (for example, dumping)		X	
False advertising	X		
Insider trading		X	
Money laundering		X	
Organizational bribe giving			X
Tax evasion	X		
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy			X
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	

FRAUD VULNERABILITY GRID—RETAIL SECTOR *(continued)*

Fraud Vulnerability Grid Retail Sector	High	Avg	Low or NA
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations	X		
Accounting reconciliations (bank, accounts receivable, accounts payable variance)	X		
Customer account statements, or confirmations, or both	X		
No management override of controls	X		
Computer Controls:			
Access restrictions (for example, physical access, passwords)	X		
Regular off-site backups of programs and data files	X		
Software controls (for example, antivirus, full documentation)	X		
Programmer controls (for example, supervision, antisabotage)	X		
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)	X		
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

13 SMALL BUSINESS

13.1 Introduction

The small business sector cuts across a large number of the other sectors. While there is no arbitrary dividing line, it is typically thought of as an owner-operated business with relatively few employees.

As with the professional services sector, the management of the small business is also the ownership. In that sense, there is more at stake here in terms of fraud losses. Once again, every dollar lost to fraud is a dollar out of the small-business person's own pocket, and not merely a management embarrassment.

13.2 Key Vulnerabilities

By far the most important vulnerability to fraud in this sector is employee fraud involving cash (for example, skimming) or accounts receivable (for example, lapping schemes). Inventory-related frauds can also be a problem.

13.3 Key Preventive Controls

Some of the key fraud prevention controls in the small business sector include:

- Enforcement (for example dismissal and prosecution for the commission of fraud by an employee).
- Fair treatment of employees. In closely-held businesses, it is important that employees not become alienated from the owner-manager, because that will only help establish a motive for fraud.
- Good physical controls over cash and inventory.
- Regular accounting reconciliations.
- Good supervisory control is perhaps the most important preventive control. This includes an awareness of the possibility of fraud, something that is absent among many small-business owners who become preoccupied with other areas of the business.
- Adequate insurance.

13.4 Checklist and Grids

A fraud risk management checklist specific to the small business sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Small Business Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the small business sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds such as cash theft, cash skimming, or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good policies especially strict enforcement)	☐	☐	☐	___
• Inventory fraud, such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good policies [especially strict enforcement])	☐	☐	☐	___
b. Have the following vulnerability areas for the small business sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable fraud, such as phony suppliers, inflated invoices, and the like (related controls include job descriptions and segregation of duties, and especially supervision)	☐	☐	☐	___
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good policies [especially strict enforcement])	☐	☐	☐	___
• Sabotage and espionage by employees, competitors or others (related controls include physical access restrictions, and good policies [particularly at the hiring stage])	☐	☐	☐	___
• Computer crime (related controls include job descriptions and segregation of duties, mandatory annual vacations, good computer integrity controls, and supervision)	☐	☐	☐	___

SMALL BUSINESS SECTOR CHECKLIST *(continued)*

Small Business Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Commercial crime by the business, including breach of trust, environmental crime, false advertising, money laundering, tax evasion, and violating occupational health and safety (OSHA) laws (related controls include good policies [especially strict enforcement and supervision])	☐	☐	☐	___

Fraud Vulnerability Grid **Small Business Sector**	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming, or lapping (front-end frauds)	X		
Accounts receivable (for example, lapping, phony customers or credits)	X		
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)			X
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like		X	
Manipulation of financial statements by principals			X
Manipulation of business valuations by principals			X
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)		X	
Environmental crime (for example, dumping)		X	
False advertising		X	
Insider trading			X
Money laundering		X	
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy			X
Corporate Policies:			
Mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)	X		

FRAUD VULNERABILITY GRID—SMALL BUSINESS SECTOR *(continued)*

Fraud Vulnerability Grid **Small Business Sector**	**High**	**Avg**	**Low or NA**
Fair performance appraisal and review system	X		
Employee screening and testing before hiring		X	
Principals acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like		X	
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)	X		
Customer account statements, or confirmations, or both		X	
No principal's override of controls			X
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)			X
Supervisory, Audit-Investigative and Insurance:			
Principal's awareness of fraud or possibility of fraud	X		
Supervisory review and approval	X		
Supervisory performance, or independent checks, or both	X		
Principal's follow-up (exceptions, customer complaints)	X		
Auditors (internal, external)		X	
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)	X		

14 Transportation

14.1 Introduction

For purposes of this section, the transportation sector includes:

- Trucking industry
- Railway and airline companies (both passenger and freight)
- Other passenger transportation systems (buses, subways, ferries, etc.)

14.2 Key Vulnerabilities

The most important vulnerability to fraud in this sector is in the billing and accounts receivable area. Accounts receivable lapping schemes, for example, are a major risk especially among smaller carriers. Cash frauds may also exist where payment by customers is in cash.

Because of the competitiveness of the industry and the fact that much of it is contract-based, there is also a higher risk of frauds involving bid rigging, kickbacks, and secret commissions.

14.3 Key Preventive Controls

Some of the key fraud prevention controls in the transportation sector include:

- Strong enforcement, including dismissal and prosecution of employees for fraud.
- Job descriptions with good segregation of duties.
- Reconciliations, especially bank and accounts receivable.
- Customer statements with supervisory follow-up on any related customer complaints or exceptions.
- A good internal audit function and periodic external audits.

14.4 Checklist and Grids

A fraud risk management checklist specific to the transportation sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Transportation Sector Checklist	**Yes**	**No**	**NA**	**Ref**
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the transportation sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds such as cash theft, cash skimming or accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies] and good corporate policies especially strict enforcement)	☐	☐	☐	___
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
b. Have the following vulnerability areas for the transportation sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Accounts payable and payroll fraud, such as phony suppliers or ghost employees (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
• Management fraud, such as false financial statements, inflating income, manipulating share prices, insider trading, and the like (related controls include good corporate policies [especially strong enforcement and strong internal audit functions])	☐	☐	☐	___
• Sabotage and espionage by employees, competitors, and the like (related controls include access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___
• Outsider frauds, such as inflated supplier invoices or product substitution, con schemes, and the like (related controls include good corporate policies and supervision)	☐	☐	☐	___

TRANSPORTATION SECTOR CHECKLIST *(continued)*

Transportation Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Computer crime (related controls include job descriptions, segregation of duties, annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___
• Commercial crime by the organization, including environmental crime, false advertising, money laundering, tax evasion, and violating occupational health and safety laws (related controls include good corporate policies, strict enforcement, supervision, and strong internal audit functions)	☐	☐	☐	___

Fraud Vulnerability Grid Transportation Sector	**High**	**Avg**	**Low or NA**
Internal Frauds:			
Cash theft, skimming or lapping (front-end frauds)	X		
Accounts receivable (for example, lapping, phony customers or credits)	X		
Inventory fraud (for example, theft, diversion)		X	
Accounts payable frauds (for example, phony suppliers)		X	
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid rigging, kickbacks, secret commissions, and the like	X		
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers		X	
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)		X	
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)			X
Environmental crime (for example, dumping)		X	
False advertising		X	
Insider trading		X	
Money laundering		X	
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy			X
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	

Fraud Vulnerability Grid—Transportation Sector *(continued)*

Fraud Vulnerability Grid Transportation Sector	High	Avg	Low or NA
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)		X	
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations		X	
Accounting reconciliations (bank, accounts receivable, accounts payable variance)	X		
Customer account statements, or confirmations, or both	X		
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)		X	
Regular off-site backups of programs and data files		X	
Software controls (for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)	X		
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

15 WHOLESALE

15.1 Introduction

The wholesale sector basically consists of distributors and importers of just about any form of merchandise. Typically, the sector is the bridge between the manufacturing and retail sectors.

15.2 Key Vulnerabilities

Employee schemes involving any one or more of the following–accounts receivable, inventory, or accounts payable–are probably the most common threats, as well as frauds by suppliers, such as overbilling and product substitution.

15.3 Key Preventive Controls

Key controls include:

- Enforcement, including dismissal and prosecution for fraud.
- Strong physical access controls over assets, especially inventory.
- Job descriptions that are clear and adhered to, including appropriate segregation of duties.
- Mandatory annual vacations. Ongoing schemes are common in this sector. These schemes often fall apart and are easily detected when the perpetrator is removed from the scene for even a few weeks.
- Regular (that is, monthly) accounting reconciliations, including bank, accounts receivable and accounts payable.
- Good computer security, especially access restrictions.
- Supervisory follow-up on exceptions and customer complaints.
- A strong internal audit function and periodic external audits.

15.4 Checklist and Grids

A fraud risk management checklist specific to the wholesale sector follows, along with related grids that highlight fraud vulnerability and key preventive controls in that sector.

Wholesale Sector Checklist	Yes	No	NA	Ref
1. Generic Checklists				
a. This checklist is designed to be used as an addendum or supplement to the generic Risk Management–Ethical Environment Checklist in chapter 2 of this Handbook, as well as the other checklists cross-referenced therein. Has the Risk Management–Ethical Environment Checklist been completed?	☐	☐	☐	___
2. Key Vulnerabilities and Controls				
a. Have the following high vulnerability areas for the wholesale sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Front-end and lapping frauds, especially accounts receivable lapping (related controls include job descriptions and segregation of duties, mandatory annual vacations, regular accounting reconciliations, follow-up of exceptions [for example, relating to customer complaints or confirmation discrepancies], and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Inventory fraud, such as theft or diversion (related controls include physical access restrictions and surveillance, periodic and surprise counts, job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Accounts payable frauds, especially phony suppliers and inflated invoices (related controls include job descriptions and segregation of duties, internal audit [especially confirmations], and supervision)	☐	☐	☐	___
b. Have the following vulnerability areas for the transportation sector, and related controls, as also set out on the attached grids, been adequately addressed:				
• Management fraud, such as false financial statements, inflating income, manipulating share prices, insider trading, and the like (related controls include good corporate policies [especially strong enforcement], and strong internal audit functions and periodic external audits)	☐	☐	☐	___
• Sabotage and espionage by employees, competitors, and the like (related controls include access restrictions, and good corporate policies [particularly at the hiring stage])	☐	☐	☐	___
• Computer crime (related controls include job descriptions, segregation of duties, annual vacations, good computer integrity controls, supervision, and a strong internal audit function)	☐	☐	☐	___

WHOLESALE SECTOR CHECKLIST *(continued)*

Wholesale Sector Checklist	**Yes**	**No**	**NA**	**Ref**
• Secret commissions, kickbacks, and the like (related controls include job descriptions and segregation of duties, supervision, and good corporate policies [especially strict enforcement])	☐	☐	☐	___
• Commercial crime by the organization, including environmental crime, false advertising, money laundering, tax evasion, and violating occupational health and safety (OSHA) laws (related controls include good corporate policies, strict enforcement, supervision, and strong internal audit functions)	☐	☐	☐	___

Fraud Vulnerability Grid Wholesale Sector	High	Avg	Low or NA
Internal Frauds:			
Cash theft, skimming or lapping (front-end frauds)		X	
Accounts receivable (for example, lapping, phony customers or credits)	X		
Inventory fraud (for example, theft, diversion)	X		
Accounts payable frauds (for example, phony suppliers)	X		
Payroll frauds (for example, ghost employees)		X	
Inflated expense reports by managers and others		X	
Bid-rigging, kickbacks, secret commissions, and the like		X	
Manipulation of financial statements by officers		X	
Manipulation of share prices by directors and officers		X	
Employee sabotage or espionage		X	
External Frauds:			
Customer theft, false instruments or claims, and the like		X	
Supplier fraud (inflated invoices, product substitution)	X		
Frauds by competitors (for example, sabotage, espionage)		X	
Con schemes or extortion by outsiders		X	
Copyright piracy, patent infringement, and the like			X
Use of Computers in Fraud		X	
Commercial Crime:			
Breach of trust (for example, theft of funds, misuse of information)			X
Environmental crime (for example, dumping)		X	
False advertising		X	
Insider trading		X	
Money laundering		X	
Organizational bribe giving		X	
Tax evasion		X	
Violating occupational health and safety (OSHA) laws		X	
Violation of privacy			X
Corporate Policies:			
Corporate mission statement and code of ethics		X	
Enforcement (for example, dismissal and prosecution for fraud)	X		
Employee relations (for example, fair compensation, counseling)		X	

FRAUD VULNERABILITY GRID—WHOLESALE SECTOR *(continued)*

Fraud Vulnerability Grid Wholesale Sector	High	Avg	Low or NA
Fair performance appraisal and review system		X	
Employee screening and testing before hiring		X	
Management acting as a good role model		X	
Basic Controls:			
Physical access restrictions (for example, locks, alarms, security)	X		
Job descriptions, segregation-duplication of duties, and the like	X		
Mandatory annual vacations	X		
Accounting reconciliations (bank, accounts receivable, accounts payable variance)	X		
Customer account statements, or confirmations, or both	X		
No management override of controls		X	
Computer Controls:			
Access restrictions (for example, physical access, passwords)	X		
Regular off-site backups of programs and data files		X	
Software controls for example, antivirus, full documentation)		X	
Programmer controls (for example, supervision, antisabotage)		X	
Supervisory, Audit-Investigative and Insurance:			
Supervisor's awareness of fraud or possibility of fraud		X	
Supervisory review and approval		X	
Supervisory performance, or independent checks, or both		X	
Supervisor follow-up (exceptions, customer complaints)	X		
Auditors (internal, external)	X		
Forensic accountants and investigators		X	
Adequate insurance (for example, fidelity, fire, liability, theft)		X	

Appendix B: SAS 82

Appendix B—

Statement on Auditing Standards (SAS) No. 82, *Consideration of Fraud in a Financial Statement Audit*

February 1997

Statement on Auditing Standards

82

Issued by the Auditing Standards Board

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Consideration of Fraud in a Financial Statement Audit

(Supersedes Statement on Auditing Standards No. 53, AICPA, Professional Standards, *vol. 1, AU sec. 316; and amends AU sec. 110, "Responsibilities and Functions of the Independent Auditor" and AU sec. 230, "Due Care in the Performance of Work" of Statement on Auditing Standards No. 1, AICPA,* Professional Standards, *vol. 1, and Statement on Auditing Standards No. 47, AICPA,* Professional Standards, *vol. 1, AU sec. 312.)*

CONTENTS OF STATEMENT

SAS No. 82
Consideration of Fraud in a Financial Statement Audit*

(Supersedes Statement on Auditing Standards No. 53, AICPA,* Professional Standards, *vol. 1, AU sec. 316; and amends AU sec. 110, "Responsibilities and Functions of the Independent Auditor" and AU sec. 230, "Due Care in the Performance of Work" of Statement on Auditing Standards No. 1, AICPA,* Professional Standards, *vol. 1, and Statement on Auditing Standards No. 47, AICPA,* Professional Standards, *vol. 1, AU sec. 312.)

Introduction

1. AU Section 110 of Statement on Auditing Standards (SAS) No. 1, *Codification of Auditing Standards and Procedures,* as amended by this Statement [appendix A] (AICPA, *Professional Standards,* vol. 1, AU sec. 110, "Responsibilities and Functions of the Independent Auditor"), states that "The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud."[1] This Statement provides guidance to auditors in fulfilling that responsibility, as it relates to fraud, in an audit of financial statements conducted in accordance with generally accepted auditing standards. Specifically, this Statement—

- Describes fraud and its characteristics (see paragraphs 3 through 10).
- Requires the auditor to specifically assess the risk of material misstatement due to fraud and provides categories of fraud risk factors to be considered in the auditor's assessment (see paragraphs 11 through 25).

* All references to AU section 110 of SAS No. 1, AU section 230 of SAS No. 1, or to SAS No. 47 "as amended by this Statement" reflect the amendments that appear in appendixes A, B, and C, respectively, in this Statement.

[1] The auditor's consideration of illegal acts and responsibility for detecting misstatements resulting from illegal acts is defined in SAS No. 54, *Illegal Acts By Clients* (AICPA, *Professional Standards,* vol. 1, AU sec. 317). For those illegal acts that are defined in that Statement as having a direct and material effect on the determination of financial statement amounts, the auditor's responsibility to detect misstatements resulting from such illegal acts is the same as that for errors (see SAS No. 47, *Audit Risk and Materiality in Conducting an Audit,* as amended by this Statement [appendix C] [AICPA, *Professional Standards,* vol. 1, AU sec. 312]) or fraud.

- Provides guidance on how the auditor responds to the results of the assessment (see paragraphs 26 through 32).
- Provides guidance on the evaluation of audit test results as they relate to the risk of material misstatement due to fraud (see paragraphs 33 through 36).
- Describes related documentation requirements (see paragraph 37).
- Provides guidance regarding the auditor's communication about fraud to management, the audit committee, and others (see paragraphs 38 through 40).

2. While this Statement focuses on the auditor's consideration of fraud in an audit of financial statements, management is responsible for the prevention and detection of fraud.[2] That responsibility is described in paragraph 3 of SAS No. 1, AU section 110, "Responsibilities and Functions of the Independent Auditor," as amended, which states, "Management is responsible for adopting sound accounting policies and for establishing and maintaining internal control that will, among other things, record, process, summarize, and report transactions consistent with management's assertions embodied in the financial statements."

Description and Characteristics of Fraud

3. Although fraud is a broad legal concept, the auditor's interest specifically relates to fraudulent acts that cause a material misstatement of financial statements. The primary factor that distinguishes fraud from error is whether the underlying action that results in the misstatement in financial statements is intentional or unintentional.[3] Two types of misstatements are relevant to the auditor's consideration of fraud in a

[2] In its October 1987 report, the National Commission on Fraudulent Financial Reporting, also known as the Treadway Commission, noted that "The responsibility for reliable financial reporting resides first and foremost at the corporate level. Top management—starting with the chief executive officer—sets the tone and establishes the financial reporting environment. Therefore, reducing the risk of fraudulent financial reporting must start with the reporting company."

[3] Intent is often difficult to determine, particularly in matters involving accounting estimates and the application of accounting principles. For example, unreasonable accounting estimates may be unintentional or may be the result of an intentional attempt to misstate the financial statements. Although the auditor has no responsibility to determine intent, the auditor's responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement is relevant in either case.

financial statement audit—misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets.[4] These two types of misstatements are described in the following paragraphs.

4. *Misstatements arising from fraudulent financial reporting* are intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. Fraudulent financial reporting may involve acts such as the following:

- Manipulation, falsification, or alteration of accounting records or supporting documents from which financial statements are prepared
- Misrepresentation in, or intentional omission from, the financial statements of events, transactions, or other significant information
- Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure

5. *Misstatements arising from misappropriation of assets* (sometimes referred to as defalcation) involve the theft of an entity's assets where the effect of the theft causes the financial statements not to be presented in conformity with generally accepted accounting principles.[5] Misappropriation can be accomplished in various ways, including embezzling receipts, stealing assets, or causing an entity to pay for goods or services not received. Misappropriation of assets may be accompanied by false or misleading records or documents and may involve one or more individuals among management, employees, or third parties.

6. Fraud frequently involves the following: (*a*) a pressure or an incentive to commit fraud and (*b*) a perceived opportunity to do so. Although specific pressures and opportunities for fraudulent financial reporting may differ from those for misappropriation of assets, these two conditions usually are present for both types of fraud. For example, fraudulent financial reporting may be committed because management is under pressure to achieve an unrealistic earnings target.

[4] Unauthorized transactions also are relevant to the auditor when they could cause a misstatement in financial statements. When such transactions are intentional and result in material misstatement of the financial statements, they would fall into one of the two types of fraud discussed in this Statement. Also see the guidance in SAS No. 54.

[5] Reference to generally accepted accounting principles includes, where applicable, a comprehensive basis of accounting other than generally accepted accounting principles as defined in SAS No. 62, *Special Reports* (AICPA, *Professional Standards*, vol. 1, AU sec. 623), paragraph 4.

Misappropriation of assets may be committed because the individuals involved are living beyond their means. A perceived opportunity may exist in either situation because an individual believes he or she could circumvent internal control.

7. Fraud may be concealed through falsified documentation, including forgery. For example, management that engages in fraudulent financial reporting might attempt to conceal misstatements by creating fictitious invoices, while employees or management who misappropriate cash might try to conceal their thefts by forging signatures or creating invalid electronic approvals on disbursement authorizations. An audit conducted in accordance with generally accepted auditing standards rarely involves authentication of documentation, nor are auditors trained as or expected to be experts in such authentication.

8. Fraud also may be concealed through collusion among management, employees, or third parties. For example, through collusion, false evidence that control activities have been performed effectively may be presented to the auditor. As another example, the auditor may receive a false confirmation from a third party who is in collusion with management. Collusion may cause the auditor to believe that evidence is persuasive when it is, in fact, false.

9. Although fraud usually is concealed, the presence of risk factors or other conditions may alert the auditor to a possibility that fraud may exist. For example, a document may be missing, a general ledger may be out of balance, or an analytical relationship may not make sense. However, these conditions may be the result of circumstances other than fraud. Documents may have been legitimately lost; the general ledger may be out of balance because of an unintentional accounting error; and unexpected analytical relationships may be the result of unrecognized changes in underlying economic factors. Even reports of alleged fraud may not always be reliable, because an employee or outsider may be mistaken or may be motivated to make a false allegation.

10. An auditor cannot obtain absolute assurance that material misstatements in the financial statements will be detected. Because of (*a*) the concealment aspects of fraudulent activity, including the fact that fraud often involves collusion or falsified documentation, and (*b*) the need to apply professional judgment in the identification and evaluation of fraud risk factors and other conditions, even a properly planned and performed audit may not detect a material misstatement resulting from fraud. Accordingly, because of the above characteristics of fraud and the

nature of audit evidence as discussed in AU section 230 of SAS No. 1, as amended by this Statement [appendix B] (AICPA, *Professional Standards,* vol. 1, AU sec. 230, "Due Professional Care in the Performance of Work"), the auditor is able to obtain only reasonable assurance that material misstatements in the financial statements, including misstatements resulting from fraud, are detected.

Assessment of the Risk of Material Misstatement Due to Fraud

11. SAS No. 22, *Planning and Supervision* (AICPA, *Professional Standards,* vol. 1, AU sec. 311), provides guidance as to the level of knowledge of the entity's business that will enable the auditor to plan and perform an audit of financial statements in accordance with generally accepted auditing standards. SAS No. 47, *Audit Risk and Materiality in Conducting an Audit,* as amended by this Statement (AICPA, *Professional Standards,* vol. 1, AU sec. 312), provides that determination of the scope of the auditing procedures is directly related to the consideration of audit risk and indicates that the risk of material misstatement of the financial statements due to fraud is part of audit risk.

12. The auditor should specifically assess the risk of material misstatement of the financial statements due to fraud and should consider that assessment in designing the audit procedures to be performed. In making this assessment, the auditor should consider fraud risk factors that relate to both (*a*) misstatements arising from fraudulent financial reporting and (*b*) misstatements arising from misappropriation of assets in each of the related categories presented in paragraphs 16 and 18.[6] While such risk factors do not necessarily indicate the existence of fraud,

[6] The auditor should assess the risk of material misstatement due to fraud regardless of whether the auditor otherwise plans to assess inherent or control risk at the maximum (see paragraphs 29 and 30 of SAS No. 47, as amended by this Statement). An auditor may meet this requirement using different categories of risk factors as long as the assessment embodies the substance of each of the risk categories described in paragraphs 16 and 18. Also, since these risk categories encompass both inherent and control risk attributes, the specific assessment of the risk of material misstatement due to fraud may be performed in conjunction with the assessment of audit risk required by SAS No. 47, paragraphs 13 through 33, as amended by this Statement, and SAS

(*continued*)

they often have been observed in circumstances where frauds have occurred.

13. As part of the risk assessment, the auditor also should inquire of management (*a*) to obtain management's understanding regarding the risk of fraud in the entity and (*b*) to determine whether they have knowledge of fraud that has been perpetrated on or within the entity. Information from these inquiries could identify fraud risk factors that may affect the auditor's assessment and related response. Some examples of matters that might be discussed as part of the inquiry are (*a*) whether there are particular subsidiary locations, business segments, types of transactions, account balances, or financial statement categories where fraud risk factors exist or may be more likely to exist and (*b*) how management may be addressing such risks.

14. Although the fraud risk factors described in paragraphs 17 and 19 below cover a broad range of situations typically faced by auditors, they are only examples. Moreover, not all of these examples are relevant in all circumstances, and some may be of greater or lesser significance in entities of different size, with different ownership characteristics, in different industries, or because of other differing characteristics or circumstances. Accordingly, the auditor should use professional judgment when assessing the significance and relevance of fraud risk factors and determining the appropriate audit response.

15. For example, in a small entity domination of management by a single individual generally does not, in and of itself, indicate a failure by management to display and communicate an appropriate attitude regarding internal control and the financial reporting process. As another example, there may be little motivation for fraudulent financial reporting by management of a privately held business when the financial statements audited are used only in connection with seasonal bank borrowings, debt covenants are not especially burdensome, and the entity has a long history of financial success consistent with the industry in which it operates. Conversely, management of a small entity with unusually rapid growth or profitability may be motivated to avoid an interruption in its growth trends, especially compared with others in its industry.

No. 55, as amended by SAS No. 78, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 319), paragraphs 27 through 38. Furthermore, the assessment of audit risk may identify the presence of additional fraud risk factors that the auditor should consider.

Risk Factors Relating to Misstatements Arising From Fraudulent Financial Reporting

16. Risk factors that relate to misstatements arising from fraudulent financial reporting may be grouped in the following three categories:

a. *Management's characteristics and influence over the control environment.* These pertain to management's abilities, pressures, style, and attitude relating to internal control and the financial reporting process.
b. *Industry conditions.* These involve the economic and regulatory environment in which the entity operates.
c. *Operating characteristics and financial stability.* These pertain to the nature and complexity of the entity and its transactions, the entity's financial condition, and its profitability.

17. The following are examples of risk factors relating to misstatements arising from fraudulent financial reporting for each of the three categories described above:

a. *Risk factors relating to management's characteristics and influence over the control environment.* Examples include —
    - A motivation for management to engage in fraudulent financial reporting. Specific indicators might include —
        - — A significant portion of management's compensation represented by bonuses, stock options, or other incentives, the value of which is contingent upon the entity achieving unduly aggressive targets for operating results, financial position, or cash flow.
        - — An excessive interest by management in maintaining or increasing the entity's stock price or earnings trend through the use of unusually aggressive accounting practices.
        - — A practice by management of committing to analysts, creditors, and other third parties to achieve what appear to be unduly aggressive or clearly unrealistic forecasts.
        - — An interest by management in pursuing inappropriate means to minimize reported earnings for tax-motivated reasons.
    - A failure by management to display and communicate an appropriate attitude regarding internal control and the financial reporting process. Specific indicators might include —
        - — An ineffective means of communicating and supporting the

entity's values or ethics, or communication of inappropriate values or ethics.

- — Domination of management by a single person or small group without compensating controls such as effective oversight by the board of directors or audit committee.
- — Inadequate monitoring of significant controls.
- — Management failing to correct known reportable conditions on a timely basis.
- — Management setting unduly aggressive financial targets and expectations for operating personnel.
- — Management displaying a significant disregard for regulatory authorities.
- — Management continuing to employ an ineffective accounting, information technology, or internal auditing staff.

- Nonfinancial management's excessive participation in, or preoccupation with, the selection of accounting principles or the determination of significant estimates.
- High turnover of senior management, counsel, or board members.
- Strained relationship between management and the current or predecessor auditor. Specific indicators might include —
  - — Frequent disputes with the current or predecessor auditor on accounting, auditing, or reporting matters.
  - — Unreasonable demands on the auditor including unreasonable time constraints regarding the completion of the audit or the issuance of the auditor's reports.
  - — Formal or informal restrictions on the auditor that inappropriately limit his or her access to people or information or his or her ability to communicate effectively with the board of directors or the audit committee.
  - — Domineering management behavior in dealing with the auditor, especially involving attempts to influence the scope of the auditor's work.
- Known history of securities law violations or claims against the entity or its senior management alleging fraud or violations of securities laws.

b. *Risk factors relating to industry conditions.* Examples include —

- New accounting, statutory, or regulatory requirements that could impair the financial stability or profitability of the entity.
- High degree of competition or market saturation, accompanied by declining margins.
- Declining industry with increasing business failures and significant declines in customer demand.
- Rapid changes in the industry, such as high vulnerability to rapidly changing technology or rapid product obsolescence.

c. *Risk factors relating to operating characteristics and financial stability.* Examples include —
- Inability to generate cash flows from operations while reporting earnings and earnings growth.
- Significant pressure to obtain additional capital necessary to stay competitive considering the financial position of the entity—including need for funds to finance major research and development or capital expenditures.
- Assets, liabilities, revenues, or expenses based on significant estimates that involve unusually subjective judgments or uncertainties, or that are subject to potential significant change in the near term in a manner that may have a financially disruptive effect on the entity — such as ultimate collectibility of receivables, timing of revenue recognition, realizability of financial instruments based on the highly subjective valuation of collateral or difficult-to-assess repayment sources, or significant deferral of costs.
- Significant related-party transactions not in the ordinary course of business or with related entities not audited or audited by another firm.
- Significant, unusual, or highly complex transactions, especially those close to year end, that pose difficult "substance over form" questions.
- Significant bank accounts or subsidiary or branch operations in tax-haven jurisdictions for which there appears to be no clear business justification.
- Overly complex organizational structure involving numerous or unusual legal entities, managerial lines of authority, or contractual arrangements without apparent business purpose.
- Difficulty in determining the organization or individual(s) that control(s) the entity.

- Unusually rapid growth or profitability, especially compared with that of other companies in the same industry.
- Especially high vulnerability to changes in interest rates.
- Unusually high dependence on debt or marginal ability to meet debt repayment requirements; debt covenants that are difficult to maintain.
- Unrealistically aggressive sales or profitability incentive programs.
- Threat of imminent bankruptcy or foreclosure, or hostile takeover.
- Adverse consequences on significant pending transactions, such as a business combination or contract award, if poor financial results are reported.
- Poor or deteriorating financial position when management has personally guaranteed significant debts of the entity.

Risk Factors Relating to Misstatements Arising From Misappropriation of Assets

18. Risk factors that relate to misstatements arising from misappropriation of assets may be grouped in the two categories below. The extent of the auditor's consideration of the risk factors in category *b* is influenced by the degree to which risk factors in category *a* are present.

a. *Susceptibility of assets to misappropriation.* These pertain to the nature of an entity's assets and the degree to which they are subject to theft.

b. *Controls.* These involve the lack of controls designed to prevent or detect misappropriations of assets.

19. The following are examples of risk factors relating to misstatements arising from misappropriation of assets for each of the two categories described above:

a. *Risk factors relating to susceptibility of assets to misappropriation*
   - Large amounts of cash on hand or processed
   - Inventory characteristics, such as small size, high value, or high demand
   - Easily convertible assets, such as bearer bonds, diamonds, or computer chips

- Fixed asset characteristics, such as small size, marketability, or lack of ownership identification

b. Risk factors relating to controls
- Lack of appropriate management oversight (for example, inadequate supervision or monitoring of remote locations)
- Lack of job applicant screening procedures relating to employees with access to assets susceptible to misappropriation
- Inadequate recordkeeping with respect to assets susceptible to misappropriation
- Lack of appropriate segregation of duties or independent checks
- Lack of appropriate system of authorization and approval of transactions (for example, in purchasing)
- Poor physical safeguards over cash, investments, inventory, or fixed assets
- Lack of timely and appropriate documentation for transactions (for example, credits for merchandise returns)
- Lack of mandatory vacations for employees performing key control functions

20. The auditor is not required to plan the audit to discover information that is indicative of financial stress of employees or adverse relationships between the entity and its employees. Nevertheless, the auditor may become aware of such information. Some examples of such information include (*a*) anticipated future employee layoffs that are known to the workforce, (*b*) employees with access to assets susceptible to misappropriation who are known to be dissatisfied, (*c*) known unusual changes in behavior or lifestyle of employees with access to assets susceptible to misappropriation, and (*d*) known personal financial pressures affecting employees with access to assets susceptible to misappropriation. If the auditor becomes aware of the existence of such information, he or she should consider it in assessing the risk of material misstatement arising from misappropriation of assets.

Consideration of Risk Factors in Assessing the Risk of Material Misstatement Due to Fraud

21. Fraud risk factors cannot easily be ranked in order of importance or combined into effective predictive models. The significance of risk factors varies widely. Some of these factors will be present in entities

where the specific conditions do not present a risk of material misstatement. Accordingly, the auditor should exercise professional judgment when considering risk factors individually or in combination and whether there are specific controls that mitigate the risk. For example, an entity may not screen newly hired employees having access to assets susceptible to theft. This factor, by itself, might not significantly affect the assessment of the risk of material misstatement due to fraud. However, if it were coupled with a lack of appropriate management oversight and a lack of physical safeguards over such assets as readily marketable inventory or fixed assets, the combined effect of these related factors might be significant to that assessment.

22. The size, complexity, and ownership characteristics of the entity have a significant influence on the consideration of relevant risk factors. For example, in the case of a large entity, the auditor ordinarily would consider factors that generally constrain improper conduct by senior management, such as the effectiveness of the board of directors, the audit committee or others with equivalent authority and responsibility, and the internal audit function. The auditor also would consider what steps had been taken to enforce a formal code of conduct and the effectiveness of the budgeting or reporting system. Furthermore, risk factors evaluated at a country-specific or business segment operating level may provide different insights than the evaluation at an entity-wide level.[7] In the case of a small entity, some or all of these considerations might be inapplicable or less important. For example, a smaller entity might not have a written code of conduct but, instead, develop a culture that emphasizes the importance of integrity and ethical behavior through oral communication and by management example.

23. SAS No. 55, as amended by SAS No. 78, *Consideration of Internal Control in a Financial Statement Audit* (AICPA, *Professional Standards,* vol. 1, AU sec. 319), requires the auditor to obtain a sufficient understanding of the entity's internal control over financial reporting to plan the audit. It also notes that such knowledge should be used to identify types of potential misstatements, consider factors that affect the risk of material misstatement, and design substantive tests. The understanding often will affect the auditor's consideration of the significance of fraud risk factors. In addition, when considering the

[7] SAS No. 47, paragraph 18, as amended by this Statement, provides guidance on the auditor's consideration of the extent to which auditing procedures should be performed at selected locations or components.

significance of fraud risk factors, the auditor may wish to assess whether there are specific controls that mitigate the risk or whether specific control deficiencies may exacerbate the risk.[8]

24. If the entity has established a program that includes steps to prevent, deter, and detect fraud, the auditor may consider its effectiveness. The auditor also should inquire of those persons overseeing such programs as to whether the program has identified any fraud risk factors.

25. The assessment of the risk of material misstatement due to fraud is a cumulative process that includes a consideration of risk factors individually and in combination. In addition, fraud risk factors may be identified while performing procedures relating to acceptance or continuance of clients and engagements,[9] during engagement planning or while obtaining an understanding of an entity's internal control, or while conducting fieldwork.[10] Also, other conditions may be identified during fieldwork that change or support a judgment regarding the assessment— such as the following:

- *Discrepancies in the accounting records,* including —
  - — Transactions not recorded in a complete or timely manner or improperly recorded as to amount, accounting period, classification, or entity policy.
  - — Unsupported or unauthorized balances or transactions.
  - — Last-minute adjustments by the entity that significantly affect financial results.
- *Conflicting or missing evidential matter,* including —
  - — Missing documents.
  - — Unavailability of other than photocopied documents when documents in original form are expected to exist.
  - — Significant unexplained items on reconciliations.

[8] SAS No. 55, as amended by SAS No. 78, paragraph 47, states that assessing control risk at below the maximum level involves identifying specific controls that are likely to prevent or detect material misstatements in those assertions, and performing tests of controls to evaluate their effectiveness.

[9] See Statement on Quality Control Standards No. 2, *System of Quality Control for a CPA Firm's Accounting and Auditing Practice* (AICPA, *Professional Standards,* vol. 2, QC sec. 20), paragraphs 14 through 16.

[10] The auditor also ordinarily obtains written representations from management concerning irregularities involving management and employees that could have a material effect on the financial statements (see SAS No. 19, *Client Representations* [AICPA, *Professional Standards,* vol. 1, AU sec. 333]).

— Inconsistent, vague, or implausible responses from management or employees arising from inquiries or analytical procedures.
— Unusual discrepancies between the entity's records and confirmation replies.
— Missing inventory or physical assets of significant magnitude.

- *Problematic or unusual relationships between the auditor and client,* including —
  — Denied access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought.[11]
  — Undue time pressures imposed by management to resolve complex or contentious issues.
  — Unusual delays by the entity in providing requested information.
  — Tips or complaints to the auditor about fraud.

The Auditor's Response to the Results of the Assessment

26. A risk of material misstatement due to fraud is always present to some degree. The auditor's response to the foregoing assessment is influenced by the nature and significance of the risk factors identified as being present. In some cases, even though fraud risk factors have been identified as being present, the auditor's judgment may be that audit procedures otherwise planned are sufficient to respond to the risk factors. In other circumstances, the auditor may conclude that the conditions indicate a need to modify procedures.[12] In these circumstances, the auditor should consider whether the assessment of the risk of material misstatement due to fraud calls for an overall response, one

[11] Denial of access to information may constitute a limitation on the scope of the audit that may require the auditor to consider qualifying or disclaiming an opinion on the financial statements (see SAS No. 58, as amended, *Reports on Audited Financial Statements* [AICPA, *Professional Standards,* vol. 1, AU sec. 508], paragraphs 22 through 32).

[12] SAS No. 47, as amended by this Statement, requires the auditor to limit audit risk to a low level that is, in the auditor's professional judgment, appropriate for expressing an opinion on the financial statements.

that is specific to a particular account balance, class of transactions or assertion, or both. The auditor also may conclude that it is not practicable to modify the procedures that are planned for the audit of the financial statements sufficiently to address the risk. In that case withdrawal from the engagement with communication to the appropriate parties may be an appropriate course of action (see paragraph 36).

Overall Considerations

27. Judgments about the risk of material misstatement due to fraud may affect the audit in the following ways:

- *Professional skepticism.* Due professional care requires the auditor to exercise professional skepticism—that is, an attitude that includes a questioning mind and critical assessment of audit evidence (see SAS No. 1, AU sec. 230, "Due Professional Care in the Performance of Work," paragraphs 7 through 9, as amended by this Statement). Some examples demonstrating the application of professional skepticism in response to the auditor's assessment of the risk of material misstatement due to fraud include (*a*) increased sensitivity in the selection of the nature and extent of documentation to be examined in support of material transactions, and (*b*) increased recognition of the need to corroborate management explanations or representations concerning material matters—such as further analytical procedures, examination of documentation, or discussion with others within or outside the entity.
- *Assignment of personnel.* The knowledge, skill, and ability of personnel assigned significant engagement responsibilities should be commensurate with the auditor's assessment of the level of risk of the engagement (see SAS No. 1 [AICPA, *Professional Standards,* vol. 1, AU sec. 210, "Training and Proficiency of the Independent Auditor," paragraph 3]). In addition, the extent of supervision should recognize the risk of material misstatement due to fraud and the qualifications of persons performing the work (see SAS No. 22, paragraph 11).
- *Accounting principles and policies.* The auditor may decide to consider further management's selection and application of significant accounting policies, particularly those related to revenue recognition, asset valuation, or capitalizing versus expensing. In this respect, the auditor may have a greater concern about whether the account-

ing principles selected and policies adopted are being applied in an inappropriate manner to create a material misstatement of the financial statements.

- *Controls.* When a risk of material misstatement due to fraud relates to risk factors that have control implications, the auditor's ability to assess control risk below the maximum may be reduced. However, this does not eliminate the need for the auditor to obtain an understanding of the components of the entity's internal control sufficient to plan the audit (see SAS No. 55, as amended by SAS No. 78). In fact, such an understanding may be of particular importance in further understanding and considering any controls (or lack thereof) the entity has in place to address the identified fraud risk factors. However, this consideration also would need to include an added sensitivity to management's ability to override such controls.

28. The nature, timing, and extent of procedures may need to be modified in the following ways:

- The *nature* of audit procedures performed may need to be changed to obtain evidence that is more reliable or to obtain additional corroborative information. For example, more evidential matter may be needed from independent sources outside the entity. Also, physical observation or inspection of certain assets may become more important. (See SAS No. 31, *Evidential Matter,* as amended [AICPA, *Professional Standards,* vol. 1, AU sec. 326], paragraphs 19 through 22.)
- The *timing* of substantive tests may need to be altered to be closer to or at year end. For example, if there are unusual incentives for management to engage in fraudulent financial reporting, the auditor might conclude that substantive testing should be performed near or at year end because it would not otherwise be possible to control the incremental audit risk associated with that risk factor. (See SAS No. 45, *Omnibus Statement on Auditing Standards—1983* [AICPA, *Professional Standards,* vol. 1, AU sec. 313, "Substantive Tests Prior to the Balance-Sheet Date"], paragraph 6.)
- The *extent* of the procedures applied should reflect the assessment of the risk of material misstatement due to fraud. For example, increased sample sizes or more extensive analytical procedures may be appropriate. (See SAS No. 39, *Audit Sampling* [AICPA, *Professional Standards,* vol. 1, AU sec. 350], paragraph 23, and SAS No. 56, *Analytical Procedures* [AICPA, *Professional Standards,* vol. 1, AU sec. 329].)

Considerations at the Account Balance, Class of Transactions, and Assertion Level

29. Specific responses to the auditor's assessment of the risk of material misstatement due to fraud will vary depending upon the types or combinations of fraud risk factors or conditions identified and the account balances, classes of transactions, and assertions they may affect. If these factors or conditions indicate a particular risk applicable to specific account balances or types of transactions, audit procedures addressing these specific areas should be considered that will, in the auditor's judgment, limit audit risk to an appropriate level in light of the risk factors or conditions identified. The following are specific examples of responses:

- Visit locations or perform certain tests on a surprise or unannounced basis — for example, observing inventory at locations where auditor attendance has not been previously announced or counting cash at a particular date on a surprise basis.
- Request that inventories be counted at a date closer to year end.
- Alter the audit approach in the current year — for example, contacting major customers and suppliers orally in addition to written confirmation, sending confirmation requests to a specific party within an organization, or seeking more and different information.
- Perform a detailed review of the entity's quarter-end or year-end adjusting entries and investigate any that appear unusual as to nature or amount.
- For significant and unusual transactions, particularly those occurring at or near year end, investigate (*a*) the possibility of related parties and (*b*) the sources of financial resources supporting the transactions.[13]
- Perform substantive analytical procedures at a detailed level. For example, compare sales and cost of sales by location and line of business to auditor-developed expectations.[14]
- Conduct interviews of personnel involved in areas in which a con-

---

[13] SAS No. 45, *Omnibus Statement on Auditing Standards—1983* (AICPA, *Professional Standards*, vol. 1, AU sec. 334, "Related Parties"), provides guidance with respect to the identification of related-party relationships and transactions, including transactions that may be outside the ordinary course of business (see paragraph 6 of SAS No. 45).

[14] SAS No. 56, *Analytical Procedures* (AICPA, *Professional Standards*, vol. 1, AU sec. 329) provides guidance on performing analytical procedures used as substantive tests.

cern about the risk of material misstatement due to fraud is present, to obtain their insights about the risk and whether or how controls address the risk.

- When other independent auditors are auditing the financial statements of one or more subsidiaries, divisions, or branches, consider discussing with them the extent of work necessary to be performed to ensure that the risk of material misstatement due to fraud resulting from transactions and activities among these components is adequately addressed.
- If the work of a specialist becomes particularly significant with respect to its potential impact on the financial statements, perform additional procedures with respect to some or all of the specialist's assumptions, methods, or findings to determine that the findings are not unreasonable or engage another specialist for that purpose. (See SAS No. 73, *Using the Work of a Specialist* [AICPA, *Professional Standards,* vol. 1, AU sec. 336], paragraph 12.)

Specific Responses — Misstatements Arising From Fraudulent Financial Reporting

30. Some examples of responses to the auditor's assessment of the risk of material misstatements arising from fraudulent financial reporting are —

- ***Revenue recognition.*** If there is a risk of material misstatement due to fraud that may involve or result in improper revenue recognition, it may be appropriate to confirm with customers certain relevant contract terms and the absence of side agreements — inasmuch as the appropriate accounting is often influenced by such terms or agreements.[15] For example, acceptance criteria, delivery

[15] SAS No. 67, *The Confirmation Process* (AICPA, *Professional Standards,* vol. 1, AU sec. 330), provides guidance about the confirmation process in audits performed in accordance with generally accepted auditing standards. Among other considerations, that guidance discusses the types of respondents from whom confirmations may be requested, and what the auditor should consider if information about the respondent's competence, knowledge, motivation, ability, or willingness to respond, or about the respondent's objectivity and freedom from bias with respect to the audited entity comes to his or her attention (AU sec. 330.27). It also provides that the auditor maintain control over the confirmation requests and responses in order to minimize the possibility that the results will be biased because of interception and alteration of the confirmation requests or responses (AU sec. 330.28). Further, when confirmation responses are other than in written communications mailed to the auditor, additional

and payment terms and the absence of future or continuing vendor obligations, the right to return the product, guaranteed resale amounts, and cancellation or refund provisions often are relevant in such circumstances.

- ***Inventory quantities.*** If a risk of material misstatement due to fraud exists in inventory quantities, reviewing the entity's inventory records may help to identify locations, areas, or items for specific attention during or after the physical inventory count. Such a review may lead to a decision to observe inventory counts at certain locations on an unannounced basis (see paragraph 29). In addition, where the auditor has a concern about the risk of material misstatement due to fraud in the inventory area, it may be particularly important that the entity counts are conducted at all locations subject to count on the same date. Furthermore, it also may be appropriate for the auditor to apply additional procedures during the observation of the count — for example, examining more rigorously the contents of boxed items, the manner in which the goods are stacked (for example, hollow squares) or labeled, and the quality (that is, purity, grade, or concentration) of liquid substances such as perfumes or specialty chemicals. Finally, additional testing of count sheets, tags or other records, or the retention of copies may be warranted to minimize the risk of subsequent alteration or inappropriate compilation.

Specific Responses — Misstatements Arising From Misappropriations of Assets

31. The auditor may have identified a risk of material misstatement due to fraud relating to misappropriation of assets. For example, the auditor may conclude that such a risk of asset misappropriation at a particular operating location is significant. This may be the case when a specific type of asset is particularly susceptible to such a risk of misappropriation — for example, a large amount of easily accessible cash, or inventory items such as jewelry, that can be easily moved and sold. Control risk may be evaluated differently in each of these situations. Thus, differing circumstances necessarily would dictate different responses.

---

evidence, such as verifying the source and contents of a facsimile response in a telephone call to the purported sender, may be required to support their validity (AU sec. 330.29).

32. Usually the audit response to a risk of material misstatement due to fraud relating to misappropriation of assets will be directed toward certain account balances and classes of transactions. Although some of the audit responses noted in paragraphs 29 and 30 may apply in such circumstances, the scope of the work should be linked to the specific information about the misappropriation risk that has been identified. For example, where a particular asset is highly susceptible to misappropriation that is potentially material to the financial statements, obtaining an understanding of the control activities related to the prevention and detection of such misappropriation and testing the operating effectiveness of such controls may be warranted. In certain circumstances, physical inspection of such assets (for example, counting cash or securities) at or near year end may be appropriate. In addition, the use of substantive analytical procedures, including the development by the auditor of an expected dollar amount, at a high level of precision, to be compared with a recorded amount, may be effective in certain circumstances.

Evaluation of Audit Test Results

33. As indicated in paragraph 25, the assessment of the risk of material misstatement due to fraud is a cumulative process and one that should be ongoing throughout the audit. At the completion of the audit, the auditor should consider whether the accumulated results of audit procedures and other observations (for example, conditions noted in paragraph 25) affect the assessment of the risk of material misstatement due to fraud he or she made when planning the audit. This accumulation is primarily a qualitative matter based on the auditor's judgment. Such an accumulation may provide further insight into the risk of material misstatement due to fraud and whether there is a need for additional or different audit procedures to be performed.

34. When audit test results identify misstatements in the financial statements, the auditor should consider whether such misstatements may be indicative of fraud.[16] If the auditor has determined that misstatements are or may be the result of fraud, but the effect of the misstatements is not material to the financial statements, the auditor nevertheless should evaluate the implications, especially those dealing

[16] See note 3.

with the organizational position of the person(s) involved. For example, fraud involving misappropriations of cash from a small petty cash fund normally would be of little significance to the auditor in assessing the risk of material misstatement due to fraud because both the manner of operating the fund and its size would tend to establish a limit on the amount of potential loss and the custodianship of such funds is normally entrusted to a relatively low-level employee.[17] Conversely, when the matter involves higher level management, even though the amount itself is not material to the financial statements, it may be indicative of a more pervasive problem. In such circumstances, the auditor should reevaluate the assessment of the risk of material misstatement due to fraud and its resulting impact on (*a*) the nature, timing, and extent of the tests of balances or transactions, (*b*) the assessment of the effectiveness of controls if control risk was assessed below the maximum, and (*c*) the assignment of personnel that may be appropriate in the circumstances.

35. If the auditor has determined that the misstatement is, or may be, the result of fraud, and either has determined that the effect could be material to the financial statements or has been unable to evaluate whether the effect is material, the auditor should —

a. Consider the implications for other aspects of the audit (see previous paragraph).

b. Discuss the matter and the approach to further investigation with an appropriate level of management that is at least one level above those involved and with senior management.

c. Attempt to obtain additional evidential matter to determine whether material fraud has occurred or is likely to have occurred, and, if so, its effect on the financial statements and the auditor's report thereon.[18]

d. If appropriate, suggest that the client consult with legal counsel.

36. The auditor's consideration of the risk of material misstatement due to fraud and the results of audit tests may indicate such a significant risk of fraud that the auditor should consider withdrawing from the engagement and communicating the reasons for withdrawal to the audit committee or others with equivalent authority and responsibility (here-

[17] However, see paragraph 38 for a discussion of the auditor's communication responsibilities.

[18] See SAS No. 58 for guidance on auditors' reports issued in connection with audits of financial statements.

after referred to as the audit committee).[19, 20] Whether the auditor concludes that withdrawal from the engagement is appropriate may depend on the diligence and cooperation of senior management or the board of directors in investigating the circumstances and taking appropriate action. Because of the variety of circumstances that may arise, it is not possible to describe definitively when withdrawal is appropriate. The auditor may wish to consult with his or her legal counsel when considering withdrawal from an engagement.

Documentation of the Auditor's Risk Assessment and Response

37. In planning the audit, the auditor should document in the working papers evidence of the performance of the assessment of the risk of material misstatement due to fraud (see paragraphs 12 through 14). Where risk factors are identified as being present, the documentation should include (*a*) those risk factors identified and (*b*) the auditor's response (see paragraphs 26 through 32) to those risk factors, individually or in combination. In addition, if during the performance of the audit fraud risk factors or other conditions are identified that cause the auditor to believe that an additional response is required (paragraph 33), such risk factors or other conditions, and any further response that the auditor concluded was appropriate, also should be documented.

---

[19] Examples of "others with equivalent authority and responsibility" may include the board of directors, the board of trustees, or the owner in owner-managed entities, as appropriate.

[20] If the auditor, subsequent to the date of the report on the audited financial statements, becomes aware that facts existed at that date which might have affected the report had the auditor then been aware of such facts, the auditor should refer to section 561 of SAS No. 1 (AICPA, *Professional Standards*, vol. 1, AU sec. 561, "Subsequent Discovery of Facts Existing at the Date of the Auditor's Report"), for guidance. Furthermore, paragraph 10 of SAS No. 7, *Communications Between Predecessor and Successor Auditors* (AICPA, *Professional Standards*, vol. 1, AU sec. 315), provides guidance regarding communication to the predecessor auditor.

Communications About Fraud to Management, the Audit Committee,[21] and Others[22]

38. Whenever the auditor has determined that there is evidence that fraud may exist, that matter should be brought to the attention of an appropriate level of management. This is generally appropriate even if the matter might be considered inconsequential, such as a minor defalcation by an employee at a low level in the entity's organization. Fraud involving senior management and fraud (whether caused by senior management or other employees) that causes a material misstatement of the financial statements should be reported directly to the audit committee. In addition, the auditor should reach an understanding with the audit committee regarding the expected nature and extent of communications about misappropriations perpetrated by lower-level employees.

39. When the auditor, as a result of the assessment of the risk of material misstatement due to fraud, has identified risk factors that have continuing control implications (whether or not transactions or adjustments that could be the result of fraud have been detected), the auditor should consider whether these risk factors represent reportable conditions relating to the entity's internal control that should be communicated to senior management and the audit committee.[23] (See SAS No. 60, *Communication of Internal Control Related Matters Noted in an Audit* [AICPA, *Professional Standards*, vol. 1, AU sec. 325].) The auditor also may wish to communicate other risk factors identified when actions can be reasonably taken by the entity to address the risk.

40. The disclosure of possible fraud to parties other than the client's senior management and its audit committee ordinarily is not part of the auditor's responsibility and ordinarily would be precluded by the auditor's ethical or legal obligations of confidentiality unless the matter is reflected in the auditor's report. The auditor should recognize, however,

[21] See note 19.

[22] The requirements to communicate noted in paragraphs 38 through 40 extend to any intentional misstatement of financial statements (see paragraph 3). However, the communication may utilize terms other than *fraud* — for example, *irregularity, intentional misstatement, misappropriation, defalcation* — if there is possible confusion with a legal definition of fraud or other reason to prefer alternative terms.

[23] Alternatively, the auditor may decide to communicate solely with the audit committee.

that in the following circumstances a duty to disclose outside the entity may exist:

a. To comply with certain legal and regulatory requirements[24]

b. To a successor auditor when the successor makes inquiries in accordance with SAS No. 7, *Communications Between Predecessor and Successor Auditors* (AICPA, *Professional Standards,* vol. 1, AU sec. 315)[25]

c. In response to a subpoena

d. To a funding agency or other specified agency in accordance with requirements for the audits of entities that receive governmental financial assistance

Because potential conflicts with the auditor's ethical and legal obligations for confidentiality may be complex, the auditor may wish to consult with legal counsel before discussing matters covered by paragraphs 38 through 40 with parties outside the client.

Effective Date

41. This Statement is effective for audits of financial statements for periods ending on or after December 15, 1997. Early application of the provisions of this Statement is permissible.

[24] These requirements include reports in connection with the termination of the engagement, such as when the entity reports an auditor change under the appropriate securities law on Form 8-K and the fraud or related risk factors constitute a "reportable event" or is the source of a "disagreement," as these terms are defined in Item 304 of Regulation S-K. These requirements also include reports that may be required, under certain circumstances, pursuant to the Private Securities Litigation Reform Act of 1995 (codified in section 10A(b)1 of the Securities Exchange Act of 1934) relating to an illegal act that has a material effect on the financial statements.

[25] In accordance with SAS No. 7, communication between predecessor and successor auditors requires the specific permission of the client.

Appendix A

Amendment to "Responsibilities and Functions of the Independent Auditor"

(Amends Statement on Auditing Standards No. 1, AICPA, Professional Standards, *vol. 1, AU sec. 110.)*

1. This amendment adds a new paragraph 2 (and renumbers the existing paragraphs 2 through 9) to include a statement of the auditor's responsibility, in an audit conducted in accordance with generally accepted auditing standards, for the detection of material misstatement in the financial statements due to fraud. The Auditing Standards Board (ASB) believes that the revised description of that presently existing responsibility is more understandable because its structure parallels the description of the auditor's responsibility contained in the auditor's standard report. The ASB also believes that inclusion of this statement in the general standards should heighten the auditor's awareness of the extent of the current responsibility in an audit for the detection of material misstatement due to fraud. New language is shown in boldface italics. The amendment is effective for audits of financial statements for periods ending on or after December 15, 1997. Early application of the provisions of this Statement is permissible.

> ***2. The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud.[1] Because of the nature of audit evidence and the characteristics of fraud, the auditor is able to obtain reasonable, but not absolute, assurance that material misstatements are detected.[2] The auditor has no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by errors or fraud, that are not material to the financial statements are detected.***

---

[1] *See SAS No. 47,* Audit Risk and Materiality in Conducting an Audit, *as amended by SAS No. 82 (AICPA,* Professional Standards, *vol. 1, AU sec, 312), and SAS No. 82,* Consideration of Fraud in a Financial Statement Audit *(AICPA,* Professional Standards, *vol. 1, AU sec. 316). The auditor's consideration of illegal acts and responsibility for detecting misstatements resulting from illegal acts is defined in SAS No. 54,* Illegal Acts By Clients *(AICPA,* Professional Standards, *vol. 1, AU sec. 317). For those illegal acts that are defined in that Statement as having a direct and material effect on the determination of financial statement amounts, the auditor's responsibility to detect misstatements resulting from such illegal acts is the same as that for error or fraud.*

[2] *See SAS No. 1,* Codification of Auditing Standards and Procedures, *as amended (AICPA,* Professional Standards, *vol. 1, AU sec. 230, "Due Professional Care in the Performance of Work," paragraphs 10 through 13).*

Appendix B

Amendment to "Due Care in the Performance of Work"

(Amends Statement on Auditing Standards No. 1, AICPA, **Professional Standards,** *vol. 1, AU sec. 230.)*

1. This amendment includes an expanded discussion of due professional care and reasonable assurance reflected in the change of the section title from "Due Care in the Performance of Work" to "Due Professional Care in the Performance of Work." The objective of these revisions is to heighten the auditor's awareness of the need for professional skepticism throughout the conduct of the audit as well as to articulate clearly the concept of reasonable assurance. New language is shown in boldface italics; deleted language is shown by strikethrough. The amendment is effective for audits of financial statements for periods ending on or after December 15, 1997. Early application of the provisions of this Statement is permissible.

1. The third general standard is:

   Due professional care is to be exercised in the ***planning and*** performance of the audit and the preparation of the report.[1]

2. This standard requires the independent auditor to ***plan and*** perform his ***or her*** work with due ***professional*** care. Due ***professional*** care imposes a responsibility upon each ~~person~~ ***professional*** within an independent auditor's organization to observe the standards of field work and reporting. ~~Exercise of due care requires critical review at every level of supervision of the work done and the judgment exercised by those assisting in the audit.~~

3. ~~A paragraph appearing in~~ *Cooley on Torts,* ***a legal treatise,*** ~~often cited by attorneys in discussing due care merits quotation here~~ ***describes the obligation for due care as follows:***

   Every man who offers his services to another and is employed assumes the duty to exercise in the employment such skill as he possesses with reasonable care and diligence. In all these employments where peculiar skill is requisite, if one offers his services, he is understood as holding himself out to the public as possessing the degree of skill commonly possessed by others in the same employment, and if his pretentions are unfounded, he commits a species of fraud upon every man who employs him in reliance on his public profession. But no man, whether skilled or unskilled, undertakes that the task he assumes shall be performed successfully, and without fault or error; he undertakes for good faith and integrity, but not for infallibility, and he is liable to his employer for negligence, bad faith, or dishonesty, but not for losses consequent upon pure errors of judgment.[2]

4. The matter of due ***professional*** care concerns what the independent auditor does and how well he ***or she*** does it. ***The quotation from*** **Cooley on Torts**

---

[1] ***This amendment revises the third general standard of the ten generally accepted auditing standards.***

[2] ***D. Haggard,*** **Cooley on Torts,** ***472 (4th ed., 1932).***

provides a source from which an auditor's responsibility for conducting an audit with due professional care can be derived. The remainder of the Statement discusses the auditor's responsibility in the context of an audit.

5. An auditor should possess "the degree of skill commonly possessed" by other auditors and should exercise it with "reasonable care and diligence" (that is, with due professional care).

6. Auditors should be assigned to tasks and supervised commensurate with their level of knowledge, skill, and ability so that they can evaluate the audit evidence they are examining. The auditor with final responsibility for the engagement should know, at a minimum, the relevant professional accounting and auditing standards and should be knowledgeable about the client.[3] *The auditor with final responsibility is responsible for the assignment of tasks to, and supervision of, assistants.*[4]

Professional Skepticism

7. Due professional care requires the auditor to exercise professional skepticism. *Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. The auditor uses the knowledge, skill, and ability called for by the profession of public accounting to diligently perform, in good faith and with integrity, the gathering and objective evaluation of evidence.*

8. Gathering and objectively evaluating audit evidence requires the auditor to consider the competency and sufficiency of the evidence. Since evidence is gathered and evaluated throughout the audit, professional skepticism should be exercised throughout the audit process.

9. The auditor neither assumes that management is dishonest nor assumes unquestioned honesty. In exercising professional skepticism, the auditor should not be satisfied with less than persuasive evidence because of a belief that management is honest.

Reasonable Assurance

10. The exercise of due professional care allows the auditor to obtain reasonable assurance *that the financial statements are free of material misstatement, whether caused by error or fraud. Absolute assurance is not attainable because of the nature of audit evidence and the characteristics of fraud. Therefore, an audit conducted in accordance with generally accepted auditing standards may not detect a material misstatement.*

11. The independent auditor's objective is to obtain sufficient competent evidential matter to provide him or her with a reasonable basis for forming an opinion. The nature of most evidence derives, in part, from the concept of selective testing of the data being audited, which involves judgment regarding both the areas to be tested and the nature, timing, and extent of the tests to be performed. In addition, judgment is required in interpreting the results

---

[3] *See SAS No. 22,* Planning and Supervision *(AICPA,* Professional Standards, *vol. 1, AU sec. 311), paragraph 7.*

[4] *See SAS No. 22, paragraph 11.*

of audit testing and evaluating audit evidence. Even with good faith and integrity, mistakes and errors in judgment can be made. Furthermore, accounting presentations contain accounting estimates, the measurement of which is inherently uncertain and depends on the outcome of future events. The auditor exercises professional judgment in evaluating the reasonableness of accounting estimates based on information that could reasonably be expected to be available prior to the completion of field work.[5] *As a result of these factors, in the great majority of cases, the auditor has to rely on evidence that is persuasive rather than convincing.*[6]

12. Because of the characteristics of fraud, particularly those involving concealment and falsified documentation (including forgery), a properly planned and performed audit may not detect a material misstatement. For example, an audit conducted in accordance with generally accepted auditing standards rarely involves authentication of documentation, nor are auditors trained as or expected to be experts in such authentication. Also, auditing procedures may be ineffective for detecting an intentional misstatement that is concealed through collusion among client personnel and third parties or among management or employees of the client.

13. Since the auditor's opinion on the financial statements is based on the concept of obtaining reasonable assurance, the auditor is not an insurer and his or her report does not constitute a guarantee. Therefore, the subsequent discovery that a material misstatement, whether from error or fraud, exists in the financial statements does not, in and of itself, evidence (a) *failure to obtain reasonable assurance,* (b) *inadequate planning, performance, or judgment,* (c) *the absence of due professional care, or* (d) *a failure to comply with generally accepted auditing standards.*

[5] *See SAS No. 57,* Auditing Accounting Estimates *(AICPA,* Professional Standards, *vol. 1, AU sec. 342), paragraph 22.*

[6] *See SAS No. 31,* Evidential Matter, *as amended (AICPA,* Professional Standards, *vol. 1, AU sec. 326).*

Appendix C

Amendment to *Audit Risk and Materiality in Conducting an Audit*

(Amends Statement on Auditing Standards No. 47, AICPA,* Professional Standards, *vol. 1, AU sec. 312.)

1. This amendment revises SAS No. 47, *Audit Risk and Materiality in Conducting an Audit,* to provide a foundation within the audit risk model for the consideration of fraud and to incorporate guidance on errors that was formerly included in SAS No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities* (AICPA, *Professional Standards,* vol. 1, AU sec. 316), which is superseded by this SAS. The revisions also (*a*) elaborate on factors an auditor should consider for an entity with multiple locations or components and (*b*) include changes to conform to the definition and description of internal control contained in SAS No. 78, *Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55* (AICPA, *Professional Standards,* vol. 1, AU sec. 319). New language is shown in boldface italics; deleted language is shown by strike-through. The amendment is effective for audits of financial statements for periods ending on or after December 15, 1997. Early application of the provisions of this Statement is permissible.

1. This Statement provides guidance on the auditor's consideration of audit risk and materiality when planning and performing an audit of financial statements in accordance with generally accepted auditing standards. Audit risk and materiality affect the application of generally accepted auditing standards, especially the standards of field work and reporting, and are reflected in the auditor's standard report. Audit risk and materiality, among other matters, need to be considered together in determining the nature, timing, and extent of auditing procedures and in evaluating the results of those procedures.

2. The existence of audit risk is recognized ~~by the statement in the auditor's standard report that the auditor obtained "reasonable assurance" about whether the financial statements are free of material misstatement.~~[+] ***in the description of the responsibilities and functions of the independent auditor that states, "Because of the nature of audit evidence and the characteristics of fraud, the auditor is able to obtain reasonable, but not absolute, assurance that material misstatements are detected."***[1] Audit risk[2] is the risk that the auditor may unknowingly fail

[+] ~~For purposes of this section, misstatements includes both errors and irregularities as defined in SAS No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities*, paragraphs 2–3.~~

[1] ***See SAS No. 1,* Codification of Auditing Standards and Procedures, *as amended by SAS No. 82 (AICPA,* Professional Standards, *vol. 1, AU sec. 110, "Responsibilities and Functions of the Independent Auditor") and SAS No. 1 (AICPA,* Professional Standards, *vol. 1, AU sec. 230, "Due Professional Care in the Performance of Work"), for a further discussion of reasonable assurance.***

[2] In addition to audit risk, the auditor is also exposed to loss or injury to his ***or her*** professional practice from litigation, adverse publicity, or other events arising in connection with (*continued*)

to appropriately modify his ***or her*** opinion on financial statements that are materially misstated.[3]

3. The concept of materiality recognizes that some matters, either individually or in the aggregate, are important for fair presentation of financial statements in conformity with generally accepted accounting principles,[4] while other matters are not important. The phrase ***in the auditor's standard report*** "present fairly, in all material respects, in conformity with generally accepted accounting principles" indicates the auditor's belief that the financial statements taken as a whole are not materially misstated.

4. Financial statements are materially misstated when they contain misstatements whose effect, individually or in the aggregate, is important enough to cause them not to be presented fairly, in all material respects, in conformity with generally accepted accounting principles. ~~Misstatements result from misapplications of generally accepted accounting principles, departures from fact, or omissions of necessary information.~~ ***Misstatements can result from errors or fraud.***[5]

5. In planning the audit, the auditor is concerned with matters that could be material to the financial statements. The auditor has no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by errors or fraud, that are not material to the financial statements are detected.

---

financial statements ~~that he has~~ audited and reported on. This exposure is present even though the auditor has performed ~~his~~ ***the*** audit in accordance with generally accepted auditing standards and has reported appropriately on those financial statements. Even if an auditor assesses this exposure as low, ~~he~~ ***the auditor*** should not perform less extensive procedures than would otherwise be appropriate under generally accepted auditing standards.

[3] This definition of audit risk does not include the risk that the auditor might erroneously conclude that the financial statements are materially misstated. In such a situation, ~~he~~ ***the auditor*** would ordinarily reconsider or extend ~~his~~ auditing procedures and request that the client perform specific tasks to reevaluate the appropriateness of the financial statements. These steps would ordinarily lead the auditor to the correct conclusion. This definition also excludes the risk of an inappropriate reporting decision unrelated to the detection and evaluation of misstatements in the financial statements, such as an inappropriate decision regarding the form of the auditor's report because of ~~an uncertainty or~~ ***a*** limitation on the scope of the audit.

[4] The concepts of audit risk and materiality ***also*** are ~~also~~ applicable to financial statements presented in conformity with a comprehensive basis of accounting other than generally accepted accounting principles; references in this Statement to financial statements presented in conformity with generally accepted accounting principles also include those presentations.

[5] ***The auditor's consideration of illegal acts and responsibility for detecting misstatements resulting from illegal acts is defined in SAS No. 54,*** **Illegal Acts By Clients** ***(AICPA, Professional Standards, vol. 1, AU sec. 317). For those illegal acts that are defined in that Statement as having a direct and material effect on the determination of financial statement amounts, the auditor's responsibility to detect misstatements resulting from such illegal acts is the same as that for errors or fraud.***

6. The term errors *refers to unintentional misstatements or omissions of amounts or disclosures in financial statements. Errors may involve—*

- *Mistakes in gathering or processing data from which financial statements are prepared.*
- *Unreasonable accounting estimates arising from oversight or misinterpretation of facts.*
- *Mistakes in the application of accounting principles relating to amount, classification, manner of presentation, or disclosure.*[6]

7. Although fraud *is a broad legal concept, the auditor's interest specifically relates to fraudulent acts that cause a misstatement of financial statements. Two types of misstatements are relevant to the auditor's consideration in a financial statement audit — misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets. These two types of misstatements are further described in SAS No. 82,* Consideration of Fraud in a Financial Statement Audit *(AICPA,* Professional Standards, *vol. 1, AU sec. 316). The primary factor that distinguishes fraud from error is whether the underlying action that results in the misstatement in financial statements is intentional or unintentional.*

8. When considering the auditor's responsibility to obtain reasonable assurance that the financial statements are free from material misstatement, there is no important distinction between errors and fraud. There is a distinction, however, in the auditor's response to detected misstatements. Generally, an isolated, immaterial error in processing accounting data or applying accounting principles is not significant to the audit. In contrast, when fraud is detected, the auditor should consider the implications for the integrity of management or employees and the possible effect on other aspects of the audit.

~~5.~~ *9.* When ~~reaching a conclusion~~ *concluding* as to whether the effect of misstatements, individually or in the aggregate, is material, an auditor ordinarily should consider their nature and amount in relation to the nature and amount of items in the financial statements under audit. For example, an amount that is material to the financial statements of one entity may not be material to the financial statements of another entity of a different size or nature. Also, what is material to the financial statements of a particular entity might change from one period to another.

~~6.~~ *10.* The auditor's consideration of materiality is a matter of professional judgment and is influenced by his ***or her*** perception of the needs of a reasonable person who will rely on the financial statements. The perceived needs of a reasonable person are recognized in the discussion of materiality in Financial Accounting Standards Board Statement of Financial Accounting Concepts No. 2, *Qualitative Characteristics of Accounting Information,* which defines materiality as "the magnitude of an omission or misstatement of accounting information that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the omission or misstatement." That discussion recognizes that materiality judgments are made in light of

[6] ***Errors do not include the effect of accounting processes employed for convenience, such as maintaining accounting records on the cash basis or the tax basis and periodically adjusting those records to prepare financial statements in conformity with generally accepted accounting principles.***

surrounding circumstances and necessarily involve both quantitative and qualitative considerations.

~~7.~~ ***11.*** As a result of the interaction of quantitative and qualitative considerations in materiality judgments, misstatements of relatively small amounts that come to the auditor's attention could have a material effect on the financial statements. For example, an illegal payment of an otherwise immaterial amount could be material if there is a reasonable possibility that it could lead to a material contingent liability or a material loss of revenue.[~~5~~ 7]

Planning the Audit

~~8.~~ ***12.*** The auditor should consider audit risk and materiality both in (*a*) planning the audit and designing auditing procedures and (*b*) evaluating whether the financial statements taken as a whole are presented fairly, in all material respects, in conformity with generally accepted accounting principles. The auditor should consider audit risk and materiality in the first circumstance to obtain sufficient competent evidential matter on which to properly evaluate the financial statements in the second circumstance.

Considerations at the Financial Statements Level[~~6~~]

~~9.~~ ***13.*** The auditor should plan the audit so that audit risk will be limited to a low level that is, in his ***or her*** professional judgment, appropriate for ~~issuing~~ ***expressing*** an opinion on the financial statements. Audit risk may be assessed in quantitative or nonquantitative terms.

~~10.~~ ***14.*** SAS No. 22, *Planning and Supervision* (AICPA, *Professional Standards*, vol. 1, AU sec. 311), requires the auditor, in planning the audit, to take into consideration, among other matters, his ***or her*** preliminary judgment about materiality levels for audit purposes.[~~5~~ 8] That judgment may or may not be quantified.

~~11.~~ ***15.*** According to SAS No. 22, the nature, timing, and extent of planning and thus of the considerations of audit risk and materiality vary with the size and complexity of the entity, the auditor's experience with the entity, and his ***or her*** knowledge of the entity's business. Certain entity-related factors also affect the nature, timing, and extent of auditing procedures with respect to specific account balances and classes of transactions and related assertions. (See paragraphs ~~17~~ ***24*** through ~~26~~ ***33***.)

16. An assessment of the risk of material misstatement (whether caused by error or fraud) should be made during planning. The auditor's understanding of internal control may heighten or mitigate the auditor's concern about the risk of material misstatement.[9] In considering audit risk, the auditor

---

[~~5~~ 7] ~~The auditor's responsibility for illegal acts is discussed in~~ ***See*** SAS No. 54, *Illegal Acts by Clients* (AICPA, *Professional Standards*, vol. 1, AU sec. 317).

[~~6~~] ~~See SAS No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities*, paragraphs 10–12, for a further discussion of the consideration of audit risk at the financial statement level.~~

[~~5~~ 8] This Statement amends SAS No. 22, *Planning and Supervision*, paragraph 3e, by substituting the words "Preliminary judgment about materiality levels" in place of the words "Preliminary estimates of materiality levels."

[9] ***See SAS No. 55, as amended by SAS No. 78,* Consideration of Internal Control in a Financial Statement Audit *(AICPA,* Professional Standards, *vol. 1, AU sec. 319).***

should specifically assess the risk of material misstatement of the financial statements due to fraud.[10] The auditor should consider the effect of these assessments on the overall audit strategy and the expected conduct and scope of the audit.

17. Whenever the auditor has concluded that there is significant risk of material misstatement of the financial statements, the auditor should consider this conclusion in determining the nature, timing, or extent of procedures; assigning staff; or requiring appropriate levels of supervision. The knowledge, skill, and ability of personnel assigned significant engagement responsibilities should be commensurate with the auditor's assessment of the level of risk for the engagement. Ordinarily, higher risk requires more experienced personnel or more extensive supervision by the auditor with final responsibility for the engagement during both the planning and the conduct of the engagement. Higher risk may cause the auditor to expand the extent of procedures applied, apply procedures closer to or as of year end, particularly in critical audit areas, or modify the nature of procedures to obtain more persuasive evidence.

18. In an audit of an entity with operations in multiple locations or components, the auditor should consider the extent to which auditing procedures should be performed at selected locations or components. The factors an auditor should consider regarding the selection of a particular location or component include (a) the nature and amount of assets and transactions executed at the location or component, (b) the degree of centralization of records or information processing, (c) the effectiveness of the control environment, particularly with respect to management's direct control over the exercise of authority delegated to others and its ability to effectively supervise activities at the location or component, (d) the frequency, timing, and scope of monitoring activities by the entity or others at the location or component, and (e) judgments about materiality of the location or component.

~~12.~~ ***19.*** In planning the audit, the auditor should use his ***or her*** judgment as to the appropriately low level of audit risk and his ***or her*** preliminary judgment about materiality levels in a manner that can be expected to provide ~~him~~, within the inherent limitations of the auditing process, ~~with~~ sufficient evidential matter to obtain reasonable assurance about whether the financial statements are free of material misstatement. Materiality levels include an overall level for each statement; however, because the statements are interrelated, and for reasons of efficiency, the auditor ordinarily considers materiality for planning purposes in terms of the smallest aggregate level of misstatements that could be considered material to any one of the financial statements. For example, if ~~he~~ ***the auditor*** believes that misstatements aggregating approximately \$100,000 would have a material effect on income but that such misstatements would have to aggregate approximately \$200,000 to materially affect financial position, it would not be appropriate for him ***or her*** to design auditing procedures that would be expected to detect misstatements only if they aggregate approximately \$200,000.

~~13.~~ ***20.*** The auditor plans the audit to obtain reasonable assurance of detecting misstatements that he ***or she*** believes could be large enough, individually or in the aggregate, to be quantitatively material to the financial statements. Although the auditor should be alert for misstatements that could be qualitatively material, it ordi-

[10] ***See SAS No. 82,*** **Consideration of Fraud in a Financial Statement Audit.**

narily is not practical to design procedures to detect them. SAS No. 31, *Evidential Matter,* ***as amended*** (AICPA, *Professional Standards,* vol. 1, AU sec. 326), states that "an auditor typically works within economic limits; the auditor's opinion, to be economically useful, must be formed within a reasonable length of time and at reasonable cost."

~~14.~~ ***21.*** In some situations, the auditor considers materiality for planning purposes before the financial statements to be audited are prepared. In other situations, ~~his~~ planning takes place after the financial statements under audit have been prepared, but ~~he~~ ***the auditor*** may be aware that they require significant modification. In both types of situations, the auditor's preliminary judgment about materiality might be based on the entity's annualized interim financial statements or financial statements of one or more prior annual periods, as long ~~as he gives~~ recognition ***is given*** to the effects of major changes in the entity's circumstances (for example, a significant merger) and relevant changes in the economy as a whole or the industry in which the entity operates.

~~15.~~ ***22.*** Assuming, theoretically, that the auditor's judgment about materiality at the planning stage was based on the same information available ~~to him~~ at the evaluation stage, materiality for planning and evaluation purposes would be the same. However, it ordinarily is not feasible for the auditor, when planning an audit, to anticipate all of the circumstances that may ultimately influence ~~his~~ judgment~~s~~ about materiality in evaluating the audit findings at the completion of the audit. Thus, ~~his~~ ***the auditor's*** preliminary judgment about materiality ordinarily will differ from ~~his~~ ***the*** judgment about materiality used in evaluating the audit findings. If significantly lower materiality levels become appropriate in evaluating ~~his~~ audit findings, the auditor should reevaluate the sufficiency of the auditing procedures he ***or she*** has performed.

~~16.~~ ***23.*** In planning auditing procedures, the auditor should also consider the nature, cause (if known), and amount of misstatements that he ***or she*** is aware of from the audit of the prior period's financial statements.

Considerations at the Individual Account-Balance or Class-of-Transactions Level

~~17.~~ ***24.*** The auditor recognizes that there is an inverse relationship between audit risk and materiality considerations. For example, the risk that a particular account balance or class of transactions and related assertions could be misstated by an extremely large amount might be very low, but the risk that it could be misstated by an extremely small amount might be very high. Holding other planning considerations equal, either a decrease in the level of audit risk that the auditor judges to be appropriate in an account balance or ***a*** class of transactions or a decrease in the amount of misstatements in the balance or class that ~~he~~ ***the auditor*** believes could be material would require the auditor to do one or more of the following: (*a*) select a more effective auditing procedure, (*b*) perform auditing procedures closer to ***year end*** ~~the balance-sheet date~~, or (*c*) increase the extent of a particular auditing procedure.

~~18.~~ ***25.*** In determining the nature, timing, and extent of auditing procedures to be applied to a specific account balance or class of transactions, the auditor should design procedures to obtain reasonable assurance of detecting misstatements that he ***or she*** believes, based on ~~his~~ ***the*** preliminary judgment about materiality, could be material, when aggregated with misstatements in other balances or classes, to the financial statements taken as a whole. Auditors use various methods to design procedures to detect such misstatements. In some cases, auditors explicitly estimate, for planning purposes, the maximum amount of misstatements in the balance or class that, when combined with misstatements in other balances or classes, could exist without causing the financial statements to be materially misstated. In other cases, auditors relate their preliminary judgment about materiality to a specific account balance or class of transactions without explicitly estimating such misstatements.

~~19.~~ ***26.*** The auditor needs to consider audit risk at the individual account-balance or class-of-transactions level because such consideration directly assists ~~him~~ in determining the scope of auditing procedures for the balance or class and related assertions. The auditor should seek to restrict audit risk at the individual balance or class level in such a way that will enable him ***or her,*** at the completion of ~~his~~ ***the*** examination, to express an opinion on the financial statements taken as a whole at an appropriately low level of audit risk. Auditors use various approaches to accomplish that objective.

~~20.~~ ***27.*** At the account-balance or class-of-transactions level, audit risk consists of (*a*) the risk (consisting of inherent risk and control risk) that the balance or class and related assertions contain misstatements ***(whether caused by error or fraud)*** that could be material to the financial statements when aggregated with misstatements in other balances or classes and (*b*) the risk (detection risk) that the auditor will not detect such misstatements. The discussion that follows describes audit risk in terms of three component risks.[8][11] The way the auditor considers these component risks and combines them involves professional judgment and depends on ~~his~~ ***the*** audit approach.

a. *Inherent risk* is the susceptibility of an assertion to a material misstatement, assuming that there are no related ~~internal~~ controls ~~structure policies or procedures~~. The risk of such misstatement is greater for some assertions and related balances or classes than for others. For example, complex calculations are more likely to be misstated than simple calculations. Cash is more susceptible to theft than an inventory of coal. Accounts consisting of amounts derived from accounting estimates pose greater risks than do accounts consisting of relatively routine, factual data. External factors also influence inherent risk. For example, technological developments might make a particular product obsolete, thereby causing inventory to be more susceptible to overstatement. In addition to those factors that are peculiar to a specific assertion for an account balance or ***a*** class of transactions, factors that relate to several or all of the balances or classes may influence the inherent risk related to an assertion for a specific balance or class. These latter factors include, for example, a lack of sufficient working capital to continue operations or a declining industry characterized by a large number of business failures. ~~(See SAS No. 53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities*, paragraph 10.)~~

b. *Control risk* is the risk that a material misstatement that could occur in an assertion will not be prevented or detected on a timely basis by the entity's internal

[8][11] The formula in the appendix (paragraph 48) to SAS No. 39, *Audit Sampling* (AICPA, *Professional Standards*, vol. 1, AU sec. 350), describes audit risk in terms of four component risks. Detection risk is presented in terms of two components: the risk that analytical procedures and other relevant substantive tests would fail to detect misstatements equal to tolerable misstatement, and the allowable risk of incorrect acceptance for the substantive test of details.

control ~~structure policies or procedures~~. That risk is a function of the effectiveness of the design and operation of internal control ~~structure policies or procedures~~ in achieving the entity's ~~broad internal control structure~~ objectives relevant to ~~an audit~~ ***preparation*** of the entity's financial statements. Some control risk will always exist because of the inherent limitations of ~~any~~ internal control ~~structure~~.

c. *Detection risk* is the risk that the auditor will not detect a material misstatement that exists in an assertion. Detection risk is a function of the effectiveness of an auditing procedure and of its application by the auditor. It arises partly from uncertainties that exist when the auditor does not examine 100 percent of an account balance or ***a*** class of transactions and partly because of other uncertainties that exist even if he ***or she*** were to examine 100 percent of the balance or class. Such other uncertainties arise because an auditor might select an inappropriate auditing procedure, misapply an appropriate procedure, or misinterpret the audit results. These other uncertainties can be reduced to a negligible level through adequate planning and supervision and conduct of a firm's audit practice in accordance with appropriate quality control standards.

~~21.~~ ***28.*** Inherent risk and control risk differ from detection risk in that they exist independently of the audit of financial statements, whereas detection risk relates to the auditor's procedures and can be changed at his ***or her*** discretion. Detection risk should bear an inverse relationship to inherent and control risk. The less the inherent and control risk the auditor believes exists, the greater the detection risk ~~he~~ ***that*** can ***be*** accep***ted.*** Conversely, the greater the inherent and control risk the auditor believes exists, the less the detection risk ~~he~~ ***that*** can ***be*** accep***ted.*** These components of audit risk may be assessed in quantitative terms such as percentages or in nonquantitative terms that range, for example, from a minimum to a maximum.

~~22.~~ ***29.*** When the auditor assesses inherent risk for an assertion related to an account balance or ***a*** class of transactions, he ***or she*** evaluates numerous factors that involve professional judgment. In doing so, ~~he~~ ***the auditor*** considers not only factors peculiar to the related assertion, but also, other factors pervasive to the financial statements taken as a whole that may also influence inherent risk related to the assertion. If an auditor concludes that the effort required to assess inherent risk for an assertion would exceed the potential reduction in the extent of ~~his~~ auditing procedures derived from such an assessment, ~~he~~ ***the auditor*** should assess inherent risk as being at the maximum when designing auditing procedures.

~~23.~~ ***30.*** The auditor also uses professional judgment in assessing control risk for an assertion related to the account balance or class of transactions. The auditor's assessment of control risk is based on the sufficiency of evidential matter obtained to support the effectiveness of internal control ~~structure policies or procedures~~ in preventing or detecting misstatements in financial statement assertions. If the auditor believes control***s*** ~~structure policies or procedures~~ are unlikely to pertain to an assertion or are unlikely to be effective, or ~~if he~~ believes that evaluating their effectiveness would be inefficient, he ***or she*** would assess control risk for that assertion at the maximum.

~~24.~~ ***31.*** The auditor might make separate or combined assessments of inherent risk and control risk. If ~~he~~ ***the auditor*** considers inherent risk or control risk, separately or in combination, to be less than the maximum, he ***or she*** should have an appropriate basis for ~~his~~ ***these*** assessments. This basis may be obtained, for example, through the use of questionnaires, checklists, instructions, or similar generalized materials and, in the case of control risk, ~~his~~ ***the*** understanding of ~~the~~ internal control ~~structure~~ and ~~his~~ ***the*** performance of suitable tests of controls. However, professional judgment is required in interpreting, adapting, or expanding such generalized material as appropriate in the circumstances.

~~25.~~ ***32.*** The detection risk that the auditor can accept in the design of auditing procedures is based on the level to which he ***or she*** seeks to restrict audit risk related to the account balance or class of transactions and on ~~his~~ ***the*** assessment of inherent and control risks. As the auditor's assessment of inherent risk and control risk decreases, the detection risk that ~~he~~ can ***be*** accept***ed*** increases. It is not appropriate, however, for an auditor to rely completely on ~~his~~ assessments of inherent risk and control risk to the exclusion of performing substantive tests of account balances and classes of transactions where misstatements could exist that might be material when aggregated with misstatements in other balances or classes.

~~26.~~ ***33.*** An audit of financial statements is a cumulative process; as the auditor performs planned auditing procedures, the evidence ~~he obtains~~ ***obtained*** may cause him ***or her*** to modify the nature, timing, and extent of other planned procedures. ***As a result of performing auditing procedures or from other sources during the audit,*** ~~I~~***i***nformation may come to the auditor's attention ~~as result of performing auditing procedures or from other sources during the audit~~ that differs significantly from the information on which ~~his~~ ***the*** audit plan was based. For example, the extent of misstatements ~~he detects~~ ***detected*** may alter ~~his~~ ***the*** judgment about the levels of inherent and control risks, and other information ~~he obtains~~ ***obtained*** about the financial statements may alter ~~his~~ ***the*** preliminary judgment about materiality. In such cases, ~~he~~ ***the auditor*** may need to reevaluate the auditing procedures he ***or she*** plans to apply, based on ~~his~~ ***the*** revised consideration of audit risk and materiality for all or certain of the account balances or classes of transactions and related assertions.

Evaluating Audit Findings

~~27.~~ ***34.*** In evaluating whether the financial statements are presented fairly, in all material respects, in conformity with generally accepted accounting principles, the auditor should aggregate misstatements that the entity has not corrected in a way that enables him ***or her*** to consider whether, in relation to individual amounts, subtotals, or totals in the financial statements, they materially misstate the financial statements taken as a whole. Qualitative considerations also influence ~~an~~ ***the*** auditor in reaching a conclusion as to whether misstatements are material.

~~28.~~ ***35.*** The aggregation of misstatements should include the auditor's best estimate of the total misstatements in the account balances or classes of transactions that he ***or she*** has examined (hereafter referred to as likely misstatement~~*~~[12]), not just the amount of misstatements ~~he~~ specifically identifie~~s~~***d*** (hereafter referred to as known misstatement).~~**~~[13] When the auditor tests an account balance or ***a*** class of trans-

~~*~~[12] See SAS No. ~~53, *The Auditor's Responsibility to Detect and Report Errors and Irregularities*,~~ ***82*, Consideration of Fraud in a Financial Statement Audit,** paragraphs ~~22–25,~~ ***33–35,*** for a further discussion of the auditor's consideration of differences between the accounting records and the underlying facts and circumstances. ~~This section~~ ***Those paragraphs*** provide~~s~~ specific guidance on the auditor's consideration of an audit adjustment that is, or may be, ~~an irregularity~~ ***the result of fraud.***

~~**~~[13] If the auditor were to examine all of the items in a balance or class, the likely misstatement applicable to recorded transactions in the balance or class would be the amount of known misstatements specifically identified.

actions and related assertions by an analytical procedure, he ***or she*** ordinarily would not specifically identify misstatements but would only obtain an indication of whether misstatement might exist in the balance or class and possibly its approximate magnitude. If the analytical procedure indicates that ***a*** misstatement might exist, but not its approximate amount, the auditor ordinarily would have to employ other procedures to enable him ***or her*** to estimate the likely misstatement in the balance or class. When an auditor uses audit sampling to test an assertion for an account balance or ***a*** class of transactions, he ***or she*** projects the amount of known misstatements ~~he~~ identified in ~~his~~ ***the*** sample to the items in the balance or class from which ~~his~~ ***the*** sample was selected. That projected misstatement, along with the results of other substantive tests, contributes to the auditor's assessment of likely misstatement in the balance or class.

~~29.~~ ***36.*** The risk of material misstatement of the financial statements is generally greater when account balances and classes of transactions include accounting estimates rather than essentially factual data because of the inherent subjectivity in estimating future events. Estimates, such as those for inventory obsolescence, uncollectible receivables, and warranty obligations, are subject not only to the unpredictability of future events but also to misstatements that may arise from using inadequate or inappropriate data or misapplying appropriate data. Since no one accounting estimate can be considered accurate with certainty, the auditor recognizes that a difference between an estimated amount best supported by the audit evidence and the estimated amount included in the financial statements may be reasonable, and such difference would not be considered to be a likely misstatement. However, if the auditor believes the estimated amount included in the financial statements is unreasonable, he ***or she*** should treat the difference between that estimate and the closest reasonable estimate as a likely misstatement and aggregate it with other likely misstatements. The auditor should also consider whether the difference between estimates best supported by the audit evidence and the estimates included in the financial statements, which are individually reasonable, indicate~~s~~ a possible bias on the part of the entity's management. For example, if each accounting estimate included in the financial statements was individually reasonable, but the effect of the difference between each estimate and the estimate best supported by the audit evidence was to increase income, the auditor should reconsider the estimates taken as a whole.

~~30.~~ ***37.*** In prior periods, likely misstatements may not have been corrected by the entity because they did not cause the financial statements for those periods to be materially misstated. Those misstatements might also affect the current period's financial statements.~~[4]~~[14] If the auditor believes that there is an unacceptably high risk that the current period's financial statements may be materially misstated when those prior-period likely misstatements that affect the current period's financial statements are considered along with likely misstatements arising in the current period, ~~he~~ ***the auditor*** should include in aggregate likely misstatement the effect on the current period's financial statements of those prior-period likely misstatements.

~~31.~~ ***38.*** If the auditor concludes, based on ~~his~~ ***the*** accumulation of sufficient evidential matter, that the aggregation of likely misstatements causes the financial

~~[4]~~[14] The measurement of the effect, if any, on the current period's financial statements of misstatements uncorrected in prior periods involves accounting considerations and is therefore not addressed in this Statement.

statements to be materially misstated, ~~he~~ ***the auditor*** should request management to eliminate the material misstatement. If the material misstatement is not eliminated, ~~he~~ ***the auditor*** should issue a qualified or ***an*** adverse opinion on the financial statements. Material misstatements may be eliminated by, for example, application of appropriate accounting principles, other adjustments in amounts, or the addition of appropriate disclosure of inadequately disclosed matters. Even though the aggregate effect of likely misstatements on the financial statements may be immaterial, the auditor should recognize that an accumulation of immaterial misstatements in the balance sheet could contribute to material misstatements of future financial statements.

~~32.~~ ***39.*** If the auditor concludes that the aggregation of likely misstatements does not cause the financial statements to be materially misstated, he ***or she*** should recognize that they could still be materially misstated ~~due to~~ ***because of*** further misstatement remaining undetected. As aggregate likely misstatement increases, the risk that the financial statements may be materially misstated also increases. ***The*** ~~A~~***a***uditor~~s~~ generally reduce~~s~~ this risk of material misstatement in planning the audit by restricting the extent of detection risk ~~they are~~ ***he or she is*** willing to accept for an assertion related to an account balance or ***a*** class of transactions. ***The*** ~~A~~***a***uditor~~s~~ ***also*** can ~~also~~ reduce this risk of material misstatement by modifying the nature, timing, and extent of planned auditing procedures on a continuous basis in performing the audit. (See paragraph ~~26~~ ***33***.) Nevertheless, if the auditor believes that such risk is unacceptably high, he ***or she*** should perform additional auditing procedures or satisfy himself ***or herself*** that the entity has adjusted the financial statements to reduce the risk of material misstatement to an acceptable level.

40. In aggregating known and likely misstatements that the entity has not corrected, pursuant to paragraphs 34 and 35, the auditor may designate an amount below which misstatements need not be accumulated. This amount should be set so that any such misstatements, either individually or when aggregated with other such misstatements, would not be material to the financial statements, after the possibility of further undetected misstatements is considered.

Effective Date

~~33.~~ ***41.*** This Statement is effective for audits of financial statements for periods beginning after June 30, 1984. ***The amendments are effective for audits of financial statements for periods ending on or after December 15, 1997.***

This Statement entitled Consideration of Fraud in a Financial Statement Audit *was adopted by the assenting votes of the fifteen members of the board, of whom three, Messrs. McElroy, Rockman, and Vice, assented with qualification.*

Messrs. McElroy, Rockman, and Vice qualify their assent for paragraphs 17 and 19, which list risk factors. They believe that it can be inferred from the Statement that the selection of appropriate risk factors is mandated by the Standard. Also, in paragraph 17, several of the risk factors are supported by specific indicators. These indicators, when taken with the risk factors, create a list of examples far too numerous for the body of a Statement.

They are concerned that, despite the fact that paragraph 14 of the Statement states that "the auditor should use professional judgment when assessing the . . . relevance of fraud risk factors," in practice, auditors may mistakenly believe that they need to consider all of the fraud risk factors in the Statement on every audit.

In practice, the auditor should apply judgment, based on "entities of different size, with different ownership characteristics, in different industries, or because of other differing characteristics or circumstances," as stated in paragraph 14 of the Statement. Further, as business practices and processes change, including the effects of technology, auditors will need to consider risk factors appropriate to changed circumstances.

Messrs. McElroy, Rockman, and Vice believe that the profession and the public would be better served by publishing fewer risk factors within the Statement and by providing example risk factors in nonauthoritative documents that can be better tailored to the circumstances, and that can change over time as new knowledge becomes available.

Auditing Standards Board (1996)

Fraud Task Force

DAVID L. LANDSITTEL, *Chair*
W. STEVE ALBRECHT
ROBERT E. FLEMING
JAMES S. GERSON
NORWOOD J. JACKSON, JR.
JOHN J. KILKEARY
JOSEPH P. LIOTTA
GLENN J. VICE

JANE M. MANCINO
Technical Manager, Audit and Attest Standards

Our thanks to Richard I. Miller, AICPA general counsel and secretary, for his contributions to the development of this SAS.

Note: *Statements on Auditing Standards are issued by the Auditing Standards Board, the senior technical body of the Institute designated to issue pronouncements on auditing matters. Rule 202 of the Institute's Code of Professional Conduct requires compliance with these standards.*

Glossary

Glossary

Abuse of trust: See *Trust, abuse of.*

Account manipulation, direct: The alteration of computer programs to obtain direct but unauthorized access to account files for the purpose of manipulation.

See also: *Computer crime.*

Account, nominee: A bank or trust account set up under an alias, an assumed name, a company name, a corporate name, or a blind trust.

Account, posting improper credits to: Concealing a fraud involving the sales and collection cycle. In this scheme, an employee posts credit memos or other noncash items, for example, a sales return or writeoff, to the customer account from which the funds were diverted.

See also: *Sales and collection cycle.*

Accounts receivable, misappropriation of: The diversion of payments received from customers. An employee may open a personal bank account with a name similar to that of the customer (for example, Acme Inc. rather than Acme Company). Customer payments can then be taken by the employee and deposited into the employee's bank account.

See also: *Sales and collection cycle.*

Acquisition and payment cycle: The sequence of accounting procedures that address the procurement of and payment for all goods and services except payroll and capital acquisitions.

See also: *Capital acquisition and repayment cycle; Payroll and personnel cycle; Procurement fraud.*

Advance-fee fraud: A scheme in which assurances of some future benefit (for example, a loan) are given to the proposed victim in return for a payment described as an advance service fee or other advance good-faith deposit (often falsely described as a "returnable" deposit).

Typical victims of advance-fee schemes are business people who cannot obtain banking services or credit from customary sources. They pay "deposits" or "fees" to others on the promise that the perpetrator will arrange loans or credit for them.

See also: *Commercial crime; Finance fraud.*

Advertising, false and misleading: Use of untrue or deceptive promotional techniques resulting in consumer fraud.

Victims are consumers who rely on the false or misleading advertising or promotion. Noteworthy practices include the following:

1. Advertising as a "sale" item an item that is actually at the regular or higher price
2. Misrepresenting the size, weight, volume, or utility of an item

3. Making false claims about an attribute that a good or service does not in fact possess
4. Misstating the true costs of a good or service through the use of confusing payment provisions or otherwise

See also: *Bait and switch; Consumer fraud.*

Allegation: In litigation, a formal assertion, claim, declaration, or statement of a party to an action, made in a pleading, setting out what that party expects to prove. In a nonlitigious situation, a concern backed by evidence that a party has committed fraud.

Anti-trust offense: An offence consisting of one or more of the following:

1. Combinations in restraint of trade, price fixing, predatory pricing or other schemes for the purpose of unlawfully driving competitors out of business.
2. Agreements among competitors to share business according to some agreed formula, for example, bid-rigging conspiracies and discriminatory pricing agreements.
3. Domination of a business area by one or a few enterprises.

Victims of anti-trust offenses are businesses and purchasers of goods or services who pay prices higher than they would if the offenses were not committed.

See also: *Price fixing; Procurement fraud; Trade, restraint of.*

Appraisal, false: False and inflated appraisal used to support a loan for an amount larger than would be granted if the true value of the property were known.

See also: *External fraud; land fraud; real estate fraud.*

Arson for profit: Intentional burning of a house or property whether one's own or another's to collect the payment from the insurance company on a claim for the loss.

See also: *Commercial crime; Insurance fraud; Property-insurance fraud.*

Auto-repair fraud: A form of consumer fraud involving maintenance services to automobiles.

Auto repair fraud falls into several categories, including the following:

1. Overcharging for labor or parts or use of shoddy or substandard parts
2. Failure to perform promised services or repairs
3. Charging for services not performed or parts not used
4. Performing services or repairs that are unnecessary or unwanted

See also: *Consumer fraud; Repair fraud.*

Backdooring: Sale of shares by "friends" of a promoter in a stock market manipulation scheme as the price rises but contrary to their agreement to sell only on his or her instructions.

See also: *Distribution network, setting up; Stock market manipulation; Warehousing.*

Bagman: The person who carries cash as a bribe to the recipient.

Bait and switch: A form of consumer fraud involving misleading advertising. A bargain (the *bait*) is advertised as an inducement to lure customers to the store where they are presented with a similar but higher priced item (the *switch*). Thus, the advertisement does not constitute a bona fide offer for sale of the merchandise in question. This scheme may be used because the advertised item is not available or is in short supply. The sales staff may try to prevent the customer from purchasing the advertised item by directing him or her to higher priced merchandise by criticizing the advertised goods.

See also: *Advertising, false and misleading; Consumer fraud.*

Banking fraud: Violations by insiders or customers of banks, trust companies or credit unions. Insider violations generally involve embezzlement or self-dealing whereby insiders lend money to themselves or to businesses in which they have an interest, take bribes to make loans or refrain from collecting loans, provide special favours to outsiders or defalcations from customer accounts. Violations by outsiders would include submitting false financial statements to induce a bank to make a loan, the use of fraudulent collateral, check kiting, and similar offenses.

Victims of banking fraud are bank depositors and shareholders, creditors, the federal government as the insurer of deposits, and surety companies that bond bank employees and officers.

See also: *Check kiting; Collateral fraud; Commercial bribery; Trust, abuse of.*

Bankruptcy fraud: Fraud against parties to a bankruptcy. Victims are usually creditors and suppliers of the failed or failing business, although managers of fraudulently operating businesses can also victimize silent partners and shareholders. The following are the two major kinds of bankruptcy fraud.

1. *Fraudulently planned bankruptcy.* The assets, credit, and viability of a business are purposely and systematically used to obtain cash, which is then hidden.
2. *Fraudulent concealment or diversion of assets in anticipation of filing for bankruptcy.* This prevents the assets from being sold for the benefit of creditors.

Planned thefts and fencing activities may be associated with either kind of bankruptcy fraud as a means of diverting assets for the purpose of converting them to cash.

See also: *Finance fraud.*

Bid rigging: A conspiracy among contractors to set the price or terms of a contract for the purpose of raising the cost to the purchaser.

See also: *Commercial crime; Procurement fraud.*

Biometrics: A method to ensure that only authorized people have access to computer systems, restricted areas, and/or equipment. It can include the checking of fingerprints, iris recognition, and hand geometry.

See also: *Computer-access control.*

Blowing off: The sale of unusually large amounts of stock during a stock market manipulation (also referred to as *blowing a position*).

See also: *Stock market manipulation.*

Boiler room: A place of business used to promote fraudulent sales of securities, charitable donations, lotteries, and so on, through telephone solicitation. Salespeople working from call lists ask victims to buy a particular product or service. They call both locally and long distance, use glibly scripted presentations and work on high commissions. Legitimate enterprises, especially charitable institutions, often mistakenly use the services of these operators and, as a result, rarely see much of the money collected in their names.

See also: *Charity and religious fraud; Securities fraud.*

Borrower misapplication of funds: Loan fraud in which a borrower, with little or no personal risk in the collateral, misapplies borrowed funds.

See also: *Loan or lending fraud.*

Bundling and unbundling claims: See *Claims, bundling and unbundling.*

Business-opportunity fraud: One of the most common but varied forms of fraud, in which the victim is offered the opportunity to make a living or to supplement his or her income by going into business, full- or part-time, or by purchasing a franchise or equipment to manufacture some item, sell merchandise, or perform some service.

Victims are generally individuals with a small pool of savings, who are enticed by the prospect of independence and/or income.

This kind of scheme ranges from being a total sham to an "opportunity" whose promised return is highly illusory. Work-at-home merchandising schemes, such as selling knitting machines or raising mink, or the sale of distributorships in cosmetics, special rug cleaning processes, and so on, are common examples of the kinds of opportunities offered in this form of fraud. The opportunity presented by the fraudster often includes the promise of "guaranteed" markets for the goods or services to be produced. This kind of fraud can turn into a pyramid scheme if victims are induced to enlist other prospective victims.

See also: *Franchise fraud; Pyramid scheme; Self-improvement scheme.*

Capital acquisition and repayment cycle: The sequence of accounting procedures whereby capital items are purchased and paid for. This process is sometimes referred to as the *financing cycle.*

See also: *Acquisition and payment cycle; Procurement fraud.*

Casualty-insurance fraud: Claims for staged accidents and false claims for real accidents submitted under a casualty-insurance policy covering personal injuries and property damage that may be sustained as the result of an accident.

See also: *Claim, accident with false; Insurance fraud; Personal-injury insurance fraud.*

Chain-referral scheme: Fraud in which the victim is induced to part with money or property on the representation that he or she will make money by persuading others to buy in.

First-tier victims usually believe that those they involve in the scheme (second-tier victims) will make money. Since second-tier victims can only make money by involving third-tier victims and so on, the scheme must eventually collapse. Generally, only the fraudster makes money; few first or second-tier victims (especially if they are honest) have a sufficient number of participating friends and acquaintances to come out whole.

One common form of chain-referral scheme is the chain-letter. A more sophisticated version is the *pyramid scheme.* Here, the victim is sold a franchise to sell both merchandise and other franchises. Profits are promised to come from both merchandise sold and commissions or "overrides" on merchandise sold by any second or later-tier victims who buy a franchise. The profits appear, therefore, to be in selling franchises rather than in selling merchandise. These schemes ultimately collapse under their own weight.

See also: *Merchandising fraud; Pyramid scheme.*

Charity and religious fraud: Fraud arising out of the fund-raising activities of charitable and/or religious groups.

Almost anyone can be the victim of this type of fraud often without knowing it. Even if the victim may later suspect the fraud, however, his or her individual loss may be so small that there is little desire to pursue the matter. The following two kinds of fraud are common.

1. *Fake charity.* Money is solicited for a nonexistent charitable organization or cause or for a charitable front set up to defraud donors.
2. *Misrepresentation of association with a charity or religious group.* Individuals solicited for donations to a legitimate charity or religious organization are not aware that most of the money collected is used to cover the cost of professional fund raisers and/or administrative overhead expenses, rather than the charity. (This is a gray area in law since professional fund raisers perform a legitimate service for which they may properly and legally be compensated).

In some instances, charitable organizations themselves are the victims of con artists who use them as a front to keep the largest part of the money collected. In other instances, the solicitation falls into a gray area where otherwise legitimate charities cover up the fact that most of the money collected goes to salaries and fund raising.

See also: *Boiler room; Sham, corporate.*

Check forgery: The copying of a check or some of its components (most often the signature) onto a fraudulent check to induce a financial institution to believe it is a bona fide check.

See also: *Check fraud.*

Check fraud: A general term for the attempted or actual negotiation of a bad check at a financial institution. Kinds of fraud in this category include: a false deposit made by a new customer, forged, altered or stolen check and check kiting.

See also: *Check kiting; New-account fraud.*

Check kiting: A kind of fraud against banks that depends for success on the length of time the banking system takes to clear checks. The most common form of check kiting involves at least two bad checks used intentionally to temporarily obtain credit. In the simplest case, the fraudster must open two bank accounts, each of which contains little or no money. The accounts are often established at different banks in different cities in order to create and take advantage of a longer clearing period. A check is then written on one account for deposit in the other. This process may be repeated within the next day or so to build up the amount the fraudster needs to carry out the scheme. Money is then withdrawn from one of the accounts before the first checks are cleared. The process can continue with multiple accounts in different cities and a constant stream of deposits and withdrawals.

Banks are victims of check kites. When first discovered, check kites often appear to have cost the bank far more than they actually have after all transactions have been analyzed, since hundreds of thousands of dollars in checks may have been circulated to steal only a few thousand dollars. In some instances, however, massive amounts have been stolen. In many cases, businesses employ check kites when they cannot get loans from banks to tide themselves over a temporary business crisis and intend to (and often do) put the money back into the accounts before the check kite is discovered. In these instances, the bank has been fraudulently induced to unwittingly grant what amounts to an interest-free loan. This form of fraud is becoming increasingly difficult to perpetrate because of the speed of electronic clearing.

See also: *Banking fraud; Check fraud.*

Churning: The buying and selling of stock for a client by a broker solely to generate commissions rather than to meet the client's investment objectives.

Claim, accident with false: An individual involved in a real accident later exaggerates the seriousness of his or her personal injuries in order to collect an excessive insurance claim.

See also: *Casualty-insurance fraud; Insurance fraud.*

Claim, false or fraudulent: Fraudulently written claim for payment for goods or services not provided as claimed. False claims may involve activities such as the following:

1. Presentation of a bogus claim or claimant; for example, ghost payrolling
2. Misrepresentation of the qualifications of an otherwise ineligible claim or claimant, for example, welfare fraud
3. Misrepresentation of the extent of payment or benefits to which a claimant is entitled, for example, overtime-pay fraud
4. Claims for reimbursement for goods and services allegedly provided to nonexistent recipients, for example, health care fraud, by service providers

The false claim will carry all the trappings of a legitimate claim and is most successfully undertaken by individuals with a thorough knowledge of the system being defrauded. The false claim will sometimes involve the cooperation of executives or officials of the entity to which the claims are submitted.

See also: *Commercial bribery; Ghost employee; Government-benefit program, fraud against; insurance fraud; Health-care fraud; Welfare fraud.*

Claims, bundling and unbundling: The practice of physicians or clinics billing a patient's health insurance provider (government or private carrier) separately for medical services performed at the same time.

See also: *Health-insurance fraud.*

Cleaning up the market: Buying up as many shares of a company as possible when they become available. (Also referred to as *taking out the market.*)

Collateral fraud: The holding, taking, or offering of defective collateral pursuant to a financial transaction. In many instances collateral fraud will be related to bank loan transactions. Beyond this, however, this kind of fraud may be encountered in connection with any transaction in which defective security is provided, such as security for private loans, non-existent accounts receivable sold or pledged to factors, and the like. In some cases, collateral used as security may not belong to the person offering it. The collateral could be stolen (for example, securities), borrowed, or already subject to an undisclosed lien or other encumbrance. Alternatively, there may be some gross misrepresentation as to the collateral's value.

Collateral frauds are typically violations of federal fraud and banking laws. There may be elements in banking or corporate violations involving self-dealing, such as when a bank officer makes a loan knowing the collateral is bad. Collateral frauds may also be involved in organized crime activities, for example, obtaining proceeds of stolen securities not by an attempted sale, which would precipitate discovery when title was transferred, but by their use as collateral for loans.

See also: *Banking fraud.*

Collusion or collusive fraud: A private agreement in which several parties plan to commit fraud against another party or organization. The group of fraudsters could be as few as two people and could include parties who are internal or external to an organization, or both. For example, collusion occurs if an internal fraudster helps an external fraudster commit a crime in return for a secret commission, kickback, or bribe.

See also: *External fraud; Internal fraud.*

Commercial bribery: A form of insider fraud or abuse of trust in which an employee or officer of a business, charitable organization, or government entity is given a bribe or some other valuable consideration to induce the employee or official to make a purchase, grant a contract, or provide some special privilege (such as a zoning variance or license).

See also: *Trust, abuse of; Procurement fraud.*

Commercial crime: A white-collar crime committed by an individual or group of individuals in a company for the benefit of that company and, indirectly, themselves.

See also: *Economic crime; External fraud; Procurement fraud; White-collar crime.*

Compartmentalization: A restriction that limits computer users' access to the specific files and programs for which they have a job-related requirement.

See also: *Computer access control.*

Computer-access control: A series of controls used to help ensure that only authorized persons are permitted to access computer systems. Controls include passwords, compartmentalization, the use of biometrics, one-time passwords, automatic log-off, time-day controls, dialback systems, requests for random personal information, and Internet authentication.

See also: *Biometrics; Compartmentalization; Computer crime; Dialback systems; Internet authentication; Information, random personal; Controls, time-day.*

Computer crime: A crime in which a computer is used either to commit a crime or as the target of crime. Crimes committed using a computer may include embezzlement, larceny, fraud, forgery, and counterfeiting. Crimes that target computers may include sabotage, vandalism, electronic burglary, wire tapping, and gaining illegal access. The most common forms of computer crime involve the manipulation of inputs and outputs.

See also: *Computer-access control.*

Computer fraud: Fraud arising out of the increasing use of the computer to maintain business and government records, such as those relating to inventories, accounts payable and receivable, and customer and payroll records. Most computer frauds are really traditional kinds of fraud that are committed by using a computer to alter electronic records rather than manually altering paper records. True computer frauds do exist, such as those involving unauthorized changes to a computer's programming, but these are relatively less common and are most often committed by technical computer people.

See also: *Computer crime.*

Computer intrusion: Unauthorized access to another organization's computers.

See also: *Computer-access control; Computer crime.*

Consumer fraud: A deception in the marketplace involving sellers' misrepresentations to buyers. Victims are consumers of all kinds, individual and institutional, public and private. Common forms of consumer fraud include the following:

1. Sale of useless goods or services, represented as beneficial, for example, "miracle face creams"
2. Misrepresentation of product performance, benefits, or safety
3. False and misleading advertising
4. Failure to service items after sale, including reneging on warranties
5. Repair fraud
6. Hidden charges with respect to financing, necessary follow-up services, and so on
7. Weights and measures violations

See also: *Advertising, false and misleading; Auto-repair fraud; Bait and switch; Chain-referral scheme; Merchandising fraud; Repair fraud; Weights and measures fraud.*

Controls, time-day: Controls that restrict access to computer systems to those times when employees are supposed to be on duty. An extension of this concept uses automated time-clock systems to deny access; the system reports a violation if access is attempted when an employee is shown as not being authorized to be present.

See also: *Computer-access control.*

Copyright piracy: The use of another's copyright or other business rights for profit without the legal right to manufacture or copy the product.

See also: *Commercial crime.*

Corruption, public or official: An abuse of trust violation involving commercial bribery, collusion with bid-rigging, avoidance of the competitive process in connection with the purchase of goods and services by government entities, self-dealing in connection with government purchases, or grants of franchise to use public property and real estate.

Most public corruption has its parallel in the private sector. Thus conflict of interest is the public equivalent of insider trading.

See also: *Commercial bribery; Procurement fraud; Government-benefit program, fraud against; Trust, abuse of.*

Coupon-redemption fraud: Cheating manufacturers or merchandisers who promote sales of their products by offering coupons that return part of the purchase price when the products are purchased.

Many manufacturers, primarily in the food business, place coupons in newspaper and magazine ads offering, for example, "15 CENTS OFF" if the product is purchased. The grocery store is supposed to redeem the coupon, and will customarily receive a service charge of about 5 cents for handling the transaction. Frauds are committed against the manufacturers by amassing large numbers of coupons and submitting them to manufacturers without any bona fide purchases of the products.

This kind of fraud involves two basic steps, as follows.

1. Collect coupons.
2. Process the coupons for redemption.

Coupons can be collected by going through large numbers of old newspapers and magazines; sometimes this is done by trash collection or waste disposal companies as a side venture. Processing for collection requires the collaboration of retail merchants and is most efficiently done with the cooperation of officials of food retail chains.

See also: *Commercial crime.*

Credit-card fraud: Fraudulent application for, extension, and use of credit cards. Victims are the issuers of the credit cards. Common credit card abuses include the following:

1. Use of stolen credit cards
2. False statements in the application for a credit card, including application under a false name
3. Making a purchase using a legitimate credit card with no intention of paying
4. Manufacture and use of fake credit cards
5. Electronic swiping of a card to capture card data later used to make unauthorized purchases

See also: *Banking fraud.*

Credit-card receipt, altered: A fraudulent increase in the amount recorded on a credit-card receipt.

See also: *Sales and collection cycle.*

Credit, false application for: False information on a credit application including overstated assets, nonexistent assets, understated or omitted liabilities, inflated revenue, and understated expenses.

See also: *External fraud; Loan or lending fraud.*

Credit rating fraud: Fraudulent application for, extension, and use of credit. Victims are generally the providers of credit. Common credit-related schemes include the following:

1. Sale of good credit ratings to high-risk applicants
2. False statements in credit applications
3. Creation of false credit accounts for the purpose of theft

The *modus operandi* of these schemes varies widely. Recently, employees of credit rating organizations have altered credit ratings for payment, sometimes using computer techniques. The creation of false financial statements is another common method. On a smaller scale is a fraud that operates like shoplifting–opening a charge account with false information in order to purchase and immediately take away goods.

See also: *Loan or lending fraud.*

Customs duty fraud: The false understatement by an importer of the value of goods to be imported to reduce the amount of customs duty paid to the government of the country into which the goods are imported.

See also: *Commercial crime; Tax and revenue violation.*

Debt-consolidation or adjustment swindle: The purported bundling of a debtor's assets and income to repay all creditors over a period of time in order to keep creditors from pressing for the immediate payment of all sums due.

There are legitimate private agencies that provide these services and they have similar workout procedures available after filing for bankruptcy.

The usual *modus operandi* is to use heavy television and newspaper advertising to lure debtors into signing up. Sometimes the perpetrators will talk creditors into waiting for their money; in other instances, they falsely tell the debtors they have been able to call the creditors off. They then take the debtors' assets and a portion of their weekly or monthly earnings, paying themselves first and (usually only after they have their entire "fee") dole out the remainder to creditors. Frequently, creditors receive little or nothing and the debtors are left minus their fees and still in debt.

See also: *Finance fraud.*

Dialback systems: A computer security system that accepts a user identification (ID) and password then hangs up and dials a predetermined number. The system is only accessible by dialing in from a set location.

See also: *Computer-access control.*

Differential association: A theory established by Edwin H. Sutherland that explains why crime is committed. There are ten principles to his theory which, in summary, asserts that a person becomes a criminal because of an excess of definitions favorable to violation of the law over definitions unfavorable to violation of the law.

Diploma mill: An outlet that grants diplomas to all people who apply for them in exchange for a hefty fee. Because the diploma mill is not accredited, the diplomas are worthless.

See also: *External fraud; Self-improvement scheme.*

Directory-advertising fraud: Fraud arising from the selling of printed mass advertising services. The following are the two basic kinds.

1. Impersonation schemes involve con artists who send bills to business enterprises resembling those customarily received; for example, purported bills from the phone company for yellow page advertising, with directions to make checks payable to entities whose names are similar to legitimate payees of the bills.
2. Another kind of scheme involves promising that advertising will appear in a publication distributed to potential customers even though distribution will actually be limited to the advertisers themselves, if the directory is printed at all.

See also: *External fraud.*

Distribution network, setting up: A term used in stock market manipulation. The network is set up with the promoter as its head and several distributors located in cities with facilities for trading the stock in question. Each distributor has access to a brokerage house's sales force which in turn has access to the floor traders who will actually be executing the trades. Via this network, the promoter has control over trading in the subject stock.

Double-indemnity fraud: The report by a beneficiary of a life insurance policy of a natural death as having been accidental in order to obtain more than the face value of the policy.

See also: *Insurance fraud; Life-insurance fraud.*

Double-pledging collateral: Fraudulently pledging the same collateral to different lenders before the related liens are recorded and registered.

See also: *External fraud; Land fraud; Real estate fraud.*

Down payments and retainers, absconding with: A fraud in which the fraudster absconds with money obtained from the victim in advance by the false promise to provide goods or services.

Economic crime: A crime that is similar to white-collar crime but broader in its scope in that it includes violent crimes committed by people without any particular occupational status.

See also: *White-collar crime.*

Economic espionage: An act in which business secrets are stolen for the benefit of another organization.

Economic extortion: A crime in which a financial benefit is sought or obtained through intimidation or persistent demands.

See also: *Commercial crime.*

Embezzlement and fiduciary fraud: The conversion to one's own use or benefit of the money or property of another, over which one has custody with which one has been entrusted or over which one exerts a fiduciary's control. Victims include institutions, businesses in general, pension funds, and beneficiaries of estates managed by fiduciaries.

See also: *Banking fraud; Insider trading; Loan or lending fraud; Trust, abuse of.*

Employment-agency fraud: Fraudulent solicitations of money or fees in order to find employment for, to guarantee the employment of, or to improve the employability of another. Victims are generally individuals seeking jobs or hoping to improve their skills in order to obtain better paying jobs. Variations of employment-related fraud include the following.

1. *Phony job agencies.* An agency solicits advance fees in order to find employment for the victim, when in fact, the service is neither provided nor is it intended to be.
2. *Job training fraud.* Money is received from victims to train them for specific employment. The training is not supplied; "guaranteed" job opportunities on completion of training do not materialize; the training is misrepresented as being "certified" or "recognized" by employers when it is not.

Energy-crisis fraud: Fraud arising out of the sale of goods or services related to energy or fuel use, saving, and production.

Victims are generally consumers interested in saving on energy costs. Energy schemes include the following.

1. *Merchandise schemes.* Sale of worthless or bogus items that do not deliver the specific benefits promised or the degree of benefit promised; for example, carburetor gadgets to save gasoline or phony solar heating systems. Often, these kinds of fraud occur because of the novelty of the items involved combined with the naiveté of the victims.
2. *Weights and measures violations.* Short weighing or measuring fuels to customers; for example, the manipulation of gas pump measuring devices or the misrepresentation of fuel types by changing octane ratings on fuel pumps.
3. *Distributors' discriminatory allocation of fuel.* Distribution to subdistributors and retailers, in consideration of commercial bribes to distributors' executives or special payments to companies with the power to make distribution, in the form of under-the-table payments or required purchases of other items, in violation of antitrust or other laws.

See also: *Antitrust offense; Commercial bribery; Merchandising fraud; Weights and measures fraud.*

Environmental abuse: Business behavior that can harm the environment. The legal system considers these acts to be crimes. The two major practices are pollution and the misuse of natural resources. Businesses commit these crimes to avoid the costs associated with compliance.

See also: *Commercial crime; Pollution and environmental protection violation.*

Ethics: Principles or standards of human conduct.

Evidence: Oral, written, or physical material presented as proof in a trial or other hearing for the purpose of convincing the trier of fact (that is, judge, jury, mediator, arbitrator, and so on) of the truth of the facts and allegations.

Expense report, false: Expense report containing any combination of overstated, fictitious, or duplicated items prepared and submitted for reimbursement to an employee.

See also: *Acquisition and payment cycle; Claim, false or fraudulent.*

Expert witness: A person possessing specialized knowledge acquired through experience, education, or training. Expert witnesses can provide opinions in court, whereas lay witnesses can only provide evidence regarding their physical experiences—what they saw, smelled, heard, tasted, or touched.

External fraud: Fraud committed against an organization by arm's-length parties.

See also: *Commercial crime; Internal fraud.*

Fictitious company, payment of invoices to: The embezzler establishes a fake entity (often with a post-office box for an address, and a name similar to that of a legitimate company) and gets the fake entity entered into company records as a legitimate vendor. The embezzler then produces invoices for the fake vendor, has them processed in the accounts payable system, and pockets the payments made to satisfy the fake invoices.

See also: *Acquisition and payment cycle; Procurement fraud; Sham, corporate.*

File-maintenance instructions, failure to enter: Failure to input information into the computer system because of an intention to deceive. For example, deliberately not updating computer files when an employee has left the firm and not removing that employee from the payroll records. This kind of "omission" might be for the purpose of creating a ghost employee.

See also: *Payroll and personnel cycle.*

File-maintenance transactions, phony: Performing file maintenance transactions such as changing a customer's address or adding a new employee to the payroll. These transactions can lay the groundwork for any number of frauds, for example, the use of ghost employees to embezzle funds.

See also: *Computer crime; Payroll and personnel cycle; Sales and collection cycle.*

Finance fraud: One of several kinds of fraud, including the following:

1. *False mortgage security.* The mortgage loan is larger than the underlying value of the property secured by the mortgage.
2. *Advance fee fraud.* The victim pays an up-front finder's fee in exchange for a promise to receive an advance on a loan.
3. *Debt consolidation scheme.* A fraudulent debt consolidation agency makes money by organizing the debtors' affairs and collecting and retaining most, if not all, the money handled on the debtor's behalf.

4. *Bankruptcy fraud.* This includes fraudulent conveyances, concealed assets, asset stripping, or fraudulently planned bankruptcy.

The victims of financial fraud are generally financial institutions.

See also: *Advance-fee fraud; Bankruptcy fraud; Commercial crime; Mortgage security, false.*

Financial-statement auditing: A methodology used by auditors to evaluate the accuracy, timeliness, and completeness of recorded business transactions through sampling, confirmation, and analytical techniques.

Financial statement, false: False information created by upper-level managers with intent to manipulate data to enhance reported profitability and thereby earn higher bonuses, impress supervisors or executives, impress stockholders or lenders, or simply to comply with the goals set by senior management. The methods of creating a false financial statement include overstating revenue, overstating assets, understating expenses, understating liabilities, and misrepresenting information in the notes to the financial statements.

See also: *Commercial crime; Securities fraud; Statement, false.*

Forensic: Material that is used in, or suitable to courts of law.

See also: *Forensic accounting; Forensic standard.*

Forensic accounting: An accounting subdiscipline that investigates alleged financial wrongdoing or damage for the purpose of providing evidence to meet the evidentiary standards of the courts. The forensic accountant also supplies expert testimony for arbitration hearings, mediation, and other business dispute resolution processes.

See also: *Forensic; Forensic standard.*

Forensic standard: The evidentiary test of the courts. Evidence must meet the standards of court admissibility and be able to withstand cross examination.

See also: *Forensic; Forensic accounting.*

Franchise fraud: Fraud in the sale or service of a franchise.

Franchise fraud generally occurs in one or more of the following ways.

1. The franchisor has no intention of honoring any of its obligations; that is, the "franchise" is a complete ruse to acquire the victim-franchisee's initial investment money.
2. The franchisor fails to provide promised goods or services essential to the success of the franchise.
3. The franchisor makes success for the franchisee either difficult or impossible by allowing too many franchises in a given market area.
4. The franchisor has misrepresented the market or demand for goods or services central to the franchise, or has misrepresented the level of skill needed to realize franchise profitability.

Item 1 is outright fraud, while items 2 to 4 represent variations that range from fraud to shady dealing and the failure to fulfill contractual obligations.

See also: *Business-opportunity fraud; Chain-referral scheme.*

Fraud: Criminal deception intended to financially benefit the deceiver. The deception must be criminal in nature and involve financial benefit.

See also: *Commercial crime; External fraud; Internal fraud.*

Fraud auditing: A methodology used by fraud auditors to find transactions that differ from the normal series of transactions and suggest irregularities that could be fraudulent.

See also: *Financial-statement auditing.*

Fraudulent disbursement: The theft (embezzlement) of a company's cash by an employee, for example, by using company checks either to withdraw cash directly or to pay personal expenses.

See also: *Acquisition and payment cycle.*

Front-end fraud: The improper direction given to a company's customers to take their business elsewhere thereby depriving the company of profits it would otherwise have earned.

See also: *Sales and collection cycle.*

Funeral fraud: A class of guilt-inducement fraud that relies on the emotional stress of victims who have lost or are about to lose loved ones through death. Victims are the relatives or friends of the deceased or terminally ill.

Funeral-related fraud often takes the form of consumer and merchandising fraud and generally involves one or more of the following practices.

1. *Relying on the guilt or anxiety of bereaved relatives.* Victims are persuaded to contract for unnecessary or unduly elaborate funeral services or merchandise.
2. *Billing for funeral expenses to include charges for services not performed.* The fraudster relies on the victim's grief to cloud his or her memory as to whether or not a particular service was performed and/or to preempt the victim's challenge of the bill for payment.
3. *Misrepresentation.* Victims are told that certain goods or services are required by law when they are not.
4. *Fraudulent contracts.* The victim is sold and pays for the future provision of goods or services the fraudster has neither the intention nor the capacity to provide; for example, the sale of nonexistent cemetery plots.

See also: *Consumer fraud; Guilt-inducement fraud; Merchandising fraud.*

Generic risk factors: Risk factors within the control of the entity protecting itself but outside the control of potential perpetrators.

Ghost employee: A payroll fraud in which the embezzler enters the name of a fictitious employee into the payroll system and receives the resulting payroll check. Fictitious employees are commonly referred to as "ghosts."

In one variation of this scheme, the names of individuals whose employment has terminated are kept on the payroll for several pay periods after they leave their jobs. The embezzler then receives the paychecks for the former employees. In another variation of the ghost payroll, the fraudster develops an overtime-pay scheme in which false claims are made for overtime work performed by bona fide employees.

Victims are generally public and private entities responsible for honoring payroll claims. Often, the ghost payroll is a device used to defraud government programs designed to provide employment for the unemployed or disadvantaged. This is closely related to welfare and unemployment insurance fraud. This device is used in cost-plus contracts to cheat government entities or by managers of sub-units in private enterprises to steal from their parent organizations.

See also: *Claim, false or fraudulent; Government-benefit program, fraud against; Payroll and personnel cycle.*

Government-benefit program, fraud against: Unlawful application for and receipt of money, property, or benefit from a public program designed to confer money, property, or benefit under specific guidelines.

Victims are federal, state, county, and municipal governments; their taxpayers; and qualified, intended beneficiaries of the programs. Typical kinds of fraud suffered by government programs include the following:

1. The misrepresentation of applicants' qualifications concerning program eligibility; for example, welfare received by ineligible people
2. False billing or vouchering for services not rendered or for nonexistent beneficiaries; for example, physician's claims under provincial health programs for patients not treated or for specific treatments not provided
3. Inflated billing, vouchering, or claiming that charges public programs more than the allowable costs; for example, housing fraud in which the cost of construction is inflated so that the builder or owner receives more than the total cost of land and buildings and avoids making the investment required by law and administrative guidelines
4. Embezzlement by employees or officials misusing their custodial or fiduciary positions to convert public funds, property, or benefits to their own use; for example, licensed dispensers of food stamps converting them to their own use
5. Use of properly obtained funds in which money, property, or benefit are used for purposes other than those for which they were intended; for example, the use of student loans for purposes other than education

See also: *Claim, false or fraudulent; Embezzlement and fiduciary fraud; Health-care fraud; Statement, false; Welfare fraud.*

Guilt-inducement fraud: Fraud perpetrated by inducing guilt or anxiety in the victim concerning a child, parent, spouse, or friend. Victims are persuaded to part with money or property in the belief that they are atoning for any "shortcomings" or fulfilling "obligations" toward another.

Guilt inducement is used in many kinds of fraud. A few examples are the following.

1. Encyclopedia salespeople induce victims to sign purchase contracts by suggesting that their children will fail at school unless the books are bought.
2. Children of deceased parents are persuaded to purchase elaborate and unnecessary funeral arrangements for fear of not giving a "decent" burial. Victims are urged to believe that their failure to make these purchases implies a lack of affection or respect for the deceased.
3. Unnecessary and imprudent expenditure for life insurance is induced by the suggestion that failure to do so implies a lack of care for spouse and children.
4. Self-improvement merchandise and facilities are marketed to victims on the basis of guilt inducements such as, "You owe it to your spouse to be as [*lovely, manly, successful, or whatever*] as you can be" or "You can only be a failure if you fail to take advantage of opportunities to improve your [*looks, job, speaking ability, or whatever*]."

See also: *Funeral fraud; Self-improvement scheme.*

Health-care fraud: This term covers numerous types of fraud in the health care industry, for example, marketing drugs without adequate testing or for which the test results have been falsified.

See also: *Commercial crime; Health-insurance fraud; Medical fraud.*

Health-insurance fraud: There are several forms of health insurance fraud, for example, mobile labs, bundling or unbundling claims, or collusion between an insured and a provider to claim health insurance for his or her own benefit.

See also: *Claims, bundling and unbundling; health-care fraud; insurance fraud.*

Home-repair or home-improvement fraud: Fraud arising from the provision of goods and services in connection with the repair, maintenance, or renovation of housing units.

Victims are generally homeowners but may also include public agencies or programs that subsidize or underwrite home purchase and ownership. Home repair or improvement fraud includes the following practices:

1. Intentionally shoddy or incompetent workmanship
2. Sale of overpriced or unfit materials or services
3. Failure to provide services or goods paid for by the customer
4. Submission of false claims for materials or work not provided
5. Misrepresentation of the need for particular materials or services to be performed
6. Misrepresentations or concealment of the costs of credit or of the nature of liens securing the payment obligations

The victim may be told that the home is in violation of building codes or in a condition substandard to the rest of the neighborhood thus lowering the value of the home or compromising the safety of the victim's family.

See also: *Consumer fraud; Merchandising fraud; Repair fraud.*

Homicide for profit: A homicide in which a victim is murdered for financial gain by the murderer or the person hiring the murderer.

See also: *Homicide fraud; Insurance fraud; Life-insurance fraud.*

Homicide fraud: A fraud in which a beneficiary of a life insurance policy murders the policy holder to collect benefits.

Income tax fraud: The evasion of a tax by any means including filing false or fraudulent returns.

See also: *External fraud.*

Inflated costs: Expenses that have been artificially inflated and invoiced when a contractor is paid on a cost-plus basis.

See also: *Commercial fraud; Procurement fraud.*

Information, random personal: Information, known only to an authorized individual, that is used as a means of identifying unauthorized log-in attempts to a computer system. The computer randomly transmits a question using this information and denies access to the user unless it receives the right answer. If several dozen questions are on file, it can be a very useful technique for stopping unauthorized computer use.

Input tampering: A computer scheme that can be accomplished by altering, forging, or fabricating computer input documents. In an entity, especially a small business with inadequate logical access control, input tampering is quite easy to accomplish.

See also: *Computer crime.*

Insider trading: Benefiting oneself or others in whom one has an interest by trading on privileged information or position. Typical situations include those in which a corporate officer or director trades in the stock of his or her company on the basis of inside information as to prospective profits or losses; bank officers lending money to themselves or businesses in which they have an interest; corporate executives or purchasing officials setting up suppliers of goods and services to contract with their companies.

See also: *Banking fraud; Commercial bribery; Securities fraud; Trust, abuse of.*

Instructions, unauthorized: Commands placed by a computer programmer into a computer program to perform unauthorized functions, for example, making payments to a vendor not on an approved list.

See also: *Computer crime.*

Insurance fraud: Fraud perpetrated by or against insurance companies. Victims may be the clients or stockholders of insurance companies or the insurer itself.

Insurance fraud breaks down into the following categories and subclasses.

1. Fraud perpetrated by insurers against clients or stockholders includes the following:
    a. Failure to provide coverage promised and paid for when claim is made
    b. Failure to compensate or reimburse fully on claims
    c. Manipulation of risk classes and high-risk policy holder categories

   d. Embezzlement or abuse of trust in management of premium funds and other assets of insurance companies

   e. Twisting, that is, illegal sales practices in which the insurer persuades customers to cancel current policies and purchase new replacement ones

2. Fraud perpetrated by policy holders against insurance providers includes the following:

   a. Filing of bogus claims for compensation or reimbursement, or of multiple claims for the same loss from different insurers, and so on

   b. Inflating reimbursable costs on claim statements

   c. Paying bribes or kickbacks to local agents to retain coverage or to obtain coverage in an improper risk category

   d. Failing to disclose information or making false statements in an application for insurance

See also: *Casualty-insurance fraud; Claim, accident with false; Claim, false or fraudulent; Double-indemnity fraud; Homicide fraud; Life-insurance fraud; Mortgage-insurance fraud; Personal-injury insurance fraud; Trust, abuse of.*

Intellectual-property theft: The theft of intellectual assets such as business plans or trade secrets.

Internal fraud: Fraud committed against an organization by its employees, officers, or directors.

See also: *External fraud.*

Internet authentication: A computerized security measure used to identify a specific Internet user and to send information across the Internet safely.

See also: *Computer-access control.*

Inventory balances, understating beginning: Fraudulent financial reporting to conceal inventory shortages or theft. A common method for understating beginning inventory is to overstate the allowance for inventory obsolescence. For example, understating may be perpetrated if there has been a change in management and current management wishes to report improved profitability.

See also: *Financial statement, false; Inventory and warehousing cycle.*

Inventory and warehousing cycle: The accounting process that deals with the purchase and warehousing of merchandise for manufacture or resale or both.

See also: *Acquisition and payment cycle.*

Investment fraud: The use of imprudent, illusory, or bogus projects or businesses to attract investors through the prospect of high rates of return.

Investment fraud generally victimizes those with a pool of liquid or convertible assets, ranging from retirees or near-retirement age people, widows and widowers, to high-income professionals and businessmen. Hallmarks of this kind of fraud may include the following.

1. The investment promises a higher-than-average rate of return.

2. The investment project is still in development, that is, the project or business is not a mature entity.
3. The buyer purchases the investment from a stranger.
4. The investment has a generalized definition of its nature and scope and lacks detailed plans for measuring any progress.
5. The object or site of the investment is geographically remote or distant from investors.
6. The seller fails to fully disclose facts that are material to the investor prior to his commitment of money.
7. The seller is not registered with the appropriate regulatory agencies, such as the Securities and Exchange Commission or a state's securities commission.
8. The seller promises special advantages such as tax benefits.

See also: *Land fraud; Ponzi scheme; Pyramid scheme; Securities fraud.*

Invoice, false: An invoice submitted by a contractor for goods not delivered or for service not performed.

See also: *Commercial crime; Procurement fraud.*

Invoice, false sales: An altered company copy of the sales invoice showing a lower sales amount than the original invoice sent to the client. The difference between the real sale amount and the adjusted lower amount is then misappropriated when payment is received.

See also: *Sales and collection cycle.*

Invoice, false supplier: A supplier's invoice is prepared and submitted for payment to the company even though no goods have been delivered, no services rendered, or the invoice shows inflated quantity, inflated value, or both.

See also: *Acquisition and payment cycle; Procurement fraud.*

Jitney: The buy/sell broker disclosed on the exchange printout is acting on behalf of another broker.

Kickback: A form of off-book fraud in which the funds used for illegal payments or transfers are not drawn from the payer's regular company bank account and the payments do not appear on the payer's books and records. In collusion with suppliers, a purchasing agent may get paid a kickback for any number of activities, including allowing the supplier to submit fraudulent billing and approving the payment, excess purchasing of property or services, or bid-rigging.

See also: *Commercial crime; Procurement fraud; Off-book fraud; Secret commission.*

Land fraud: The sale of land, based on extensive misrepresentations as to value, quality, facilities, and/or state of development.

Victims are usually individuals buying land for retirement and/or investment. Land fraud usually consists of the direct sale of land or the sale of an interest in land–

1. To which the seller has no present title or claim of right; that is, the seller cannot properly transfer title or interest to the buyer as represented at the time of the sale.
2. About which there has been a misrepresentation or failure to disclose a material fact.
3. At inflated or unjustified prices based on misrepresentations made to the purchaser.
4. On the promise of future performance or development, which the seller neither intends to provide nor can reasonably expect to occur. Misrepresentations usually claim the presence of utilities, water, roads, recreational facilities, credit terms, and so on.

See also: *Investment fraud.*

Landlord-tenant fraud: Unlawful leasing or renting of property. Common fraud practices by landlords include the following:

1. Keeping two sets of books, in support of tax fraud
2. Schemes to avoid the return of security deposits
3. Rental of property to which one has no title claim or right
4. Deliberate and persistent violations of safety and health regulations; failure to provide heat, services, and so on.

Lapping: A customer's payment is embezzled and then recorded as paid sometime after the receipt of a subsequent payment from another customer. To keep customer *A* from complaining, the payment from customer *B* is applied to customer *A*'s account. Customer *C*'s payment is applied to customer *B*'s account, and so on.

See also: *Sales and collection cycle.*

Legitimate front: A form of money laundering in which a legitimate front business operating with large cash receipts is opened so that illegally earned money can be mingled with the bank deposits of the legitimate income of the business to disguise the source of the illegal money.

See also: *Money laundering.*

Life-insurance fraud: Any form of fraud making a life insurance company the victim.

See also: *Double-indemnity fraud; Homicide fraud.*

Loan fraud, single-family housing: Misapplication of funds by a borrower who purchases single-family housing units, ostensibly for personal use, but in reality is purchasing rental properties for resale.

See also: *Loan or lending fraud.*

Loan or lending fraud: The use of false information or the omission of material information for the purpose of granting or extending a loan.

When perpetrated by borrowers, loan fraud may take on any of the following forms:

1. Obtaining a loan through false statements
2. Using the loan for a purpose other than that for which the loan was granted
3. Larceny by false pretenses by which a loan is obtained with no intention of repayment

When perpetrated by the lending officer, loan fraud may take on any of the following forms:

1. Lending to oneself through ghost accounts
2. Lending to friends or entities in which one has an interest
3. Commercial bribery, meaning, approving loans to those who would not otherwise qualify as borrowers in exchange for kickbacks or other considerations
4. Advance fee schemes by which would-be borrowers remit money to secure a loan that is not forthcoming or for which no payment was necessary

A separate and important dimension of loan fraud involves the misuse or misrepresentation of items of collateral and collateral accounts.

See also: *Banking fraud; Collateral fraud; Statement, false; Trust, abuse of.*

Loan, nominee: A loan made in the name of a straw borrower or agent while the identity of the real borrower is undisclosed to the lender.

Loan to non-existent borrower fraud: Use of a false identity to obtain a loan. This scheme can be carried out individually by the borrower or with the assistance of an insider such as a loan officer.

See also: *External fraud; Loan or lending fraud.*

Long the stock: Buying stock. Your long position represents the number of shares owned (also referred to as *going long*).

Market manipulation: The intentional inflation of a stock price accomplished by stock purchases, usually in a small-cap market, with a sudden sale to third parties who are left with stock that is worth substantially less than they paid for it.

Medicaid-Medicare fraud: Fraudulent practices involving the receipt or provision of health-care services under government-financed Medicare or Medicaid programs. This kind of fraud is usually perpetrated by health-care providers (both professional and facility operators) against the government financing the programs or the intended beneficiaries of the programs, or both. Specific Medicaid-Medicare fraud practices include the following.

1. *Ping-ponging.* Referring patients to other doctors in a clinic to claim reimbursement for the "consultation" rather than for bona fide patient treatment or observation.
2. *Upgrading.* Billing for services not provided.
3. *Steering.* Sending patients to a particular pharmacy, medical lab, and so on, for required prescriptions or services and receiving improper payments in return.
4. *Shorting.* Delivering less medication (for example, pills) than prescribed while charging for full amount.
5. *Procurement abuses.* Establishing supply-purchase arrangements with firms that pay kickbacks to health care facilities or providers with firms that are owned by those controlling the facility itself.

6. *False claims.* Submitting claims for payment by the government for patients who do not exist, or who were never seen or treated.

See also: *Claim, false or fraudulent; Government-benefit program, fraud against; Kickback; Procurement fraud.*

Medical fraud: Provision and sale of bogus, highly questionable or dangerous medical services, cures, or medications.

Victims are often terminally or incurably ill patients seeking miracles. Also victimized are the poorly informed, who are vulnerable to false claims for beauty treatments and cosmetics.

Medical fraud generally includes one or more of the following.

1. *Quackery.* False representation of oneself as a legally trained and licensed health care professional
2. *Fake cures.* Sale of bogus or highly questionable "cures" for specific illnesses or diseases
3. *Misrepresentation.* In addition to misrepresenting the therapeutic value of medication, the intentional omission of the known side effects of medication
4. *Misrepresentation of treatment.* False statement about the therapeutic value of a particular treatment and the degree of its "acceptance" in bona fide medical practice; omission of material information concerning known side effects of a treatment that would affect the patient's choice of treatment program

See also: *Health-care fraud.*

Merchandising fraud: An umbrella term for a broad variety of consumer fraud involving false inducements to purchase merchandise, which either is not as represented or will never be delivered.

These kinds of fraud usually involve one or more of the following:

1. Representation that the item is sold at a lower than usual price, even though it is actually sold at the usual retail price or higher
2. Misrepresentation of the quality or utility of the merchandise
3. Misrepresentation of the ultimate price or credit terms
4. Misleading information on warranties, the return policy or the validity of "money back guarantees"
5. Solicitation of money with no intention to deliver the merchandise promised
6. "Bait and switch" fraud

Victims customarily buy from door-to-door salespeople or are entrapped when they respond to newspaper, magazine, telephone, radio, or television advertisements.

See also: *Consumer fraud.*

Mixing of funds: Commingling client funds with the funds of the brokerage firm, which then enables the broker to post the winning trades to the brokerage firm or the losing trades to their clients.

See also: *Commercial crime; Securities fraud.*

Mobile lab: A scheme in which a group of people posing as medical professionals set up a lab in a storefront located in a blue-collar, low-income area to offer free physicals to people who have medical insurance. The insured is subjected to extensive, expensive tests that are billed to his or her insurance company. The mobile labs are gone when the insured returns for the test results.

See also: *Health-insurance fraud; Insurance fraud.*

Modeling-school fraud: Fraudulent schools tell students they must have a portfolio of portraits to send to potential customers in order to get modeling assignments. The victim is then charged greatly inflated prices by a photographer who is often a participant in the scam.

See also: *External fraud; Self-improvement scheme.*

Money laundering: The process of turning "dirty" money, that is, illegally obtained money, into "clean" money to conceal its existence, source or use, or to obstruct investigative efforts, to preserve assets from forfeiture or to evade taxes.

See also: *Legitimate front; Offshore banks and tax havens; Reporting guidelines, breach of; Smurfing.*

Money-transfer fraud: Funds are stolen by an outsider or bank employee with access to the correct identification numbers needed to transfer funds by wire.

See also: *External fraud.*

Mortgage-insurance fraud: A scheme in which a healthy individual, who has a mortgage insurance policy that guarantees mortgage payments to the lender if the purchaser of the property defaults because of death or disability, falsely claims that he or she is disabled in order to have the insurance company pay the mortgage.

See also: *Casualty-insurance fraud; Insurance fraud.*

Mortgage security, false: Security offered for mortgage financing purposes that is nonexistent or has a value far lower than represented.

See also: *Commercial crime; Finance fraud.*

New-account fraud: The use of false identification to open new accounts and steal money before the bank collects the funds from fresh deposits.

See also: *Check fraud.*

Nominee account: See *Account, nominee.*

Nursing-home fraud: Various kinds of fraud perpetrated by individuals providing institutional nursing and convalescent care to patients, particularly the aged.

Victims are the patients of the facilities, their families, and/or governmental entities that subsidize the cost of care.

Forms of nursing home fraud abuses include the following:

1. Unlawful conversion or attachment of patients' assets
2. False claims to patient, family, or government entity regarding services delivered

3. False statements in license applications or renewals
4. Maintenance of fraudulent records as to general or overhead costs of operation of facilities as a basis for false claims to governmental entities
5. Receipt of kickbacks from facility suppliers
6. Employment of inadequate or unqualified staff in violation of licensing guidelines

See also: *Claim, false or fraudulent; Embezzlement and fiduciary fraud; Government-benefit program, fraud against; Health-care fraud; Procurement fraud.*

Off-book fraud: Fraud that occurs outside the accounting environment where no audit trail is likely to exist.

See also: *On-book fraud.*

Offshore banks and tax havens: Banks or financial institutions located in tax havens that conduct local and international business transactions in which money and other securities can be held or transferred from one jurisdiction to another in secrecy under the protection of banking privileges. The owners of the assets direct the transactions—personally or through an intermediary, such as a trust to minimize taxes, evade taxes, or avoid creditors.

See also: *Money laundering.*

On-book fraud: Fraud occurring in a business in which an audit trail (sometimes obscure) exists that could aid in its detection.

See also: *Off-book fraud.*

Overhead charge, false: Fraudulently inflating costs through the addition of bogus labor charges or overbilling of materials to increase profits in a cost-plus contract to allow the contractor to keep the difference between actual and inflated costs.

See also: *Property-improvement fraud.*

Patent fraud: A variation of the advance fee fraud. The fraudster solicits "patentable" ideas or gadgets through newspaper advertisements, and so on, for "evaluation by experts." The "evaluation" usually involves a fee, or at least "further processing" of the submission may involve a fee. The fraudster usually has neither the intention nor the capacity to evaluate or process a patentable item.

See also: *Advance-fee fraud; Self-improvement scheme; Vanity-publishing scheme.*

Payroll and personnel cycle: The accounting process that handles the hiring, firing, and payment of employees along with timekeeping, expense accounts, and travel reimbursement and insurance matters.

See also: *Acquisition and payment cycle.*

Pension-fund fraud: Theft and fraudulent conversion of pension fund assets either by trustees, employers, or employees.

Fraud perpetuated by trustees in violation of their fiduciary duty in the management of pension funds through the following:

1. Poor investments tied to self-dealing or commercial bribery
2. Embezzlement

This fraud victimizes both the individuals who have contributed to the fund and those intending to benefit from it. Victims are employees whose potential benefits are reduced either by fraud or bankruptcy, as well as the employer whose contributions to the pension plan could be inflated or lost.

See also: *Embezzlement and fiduciary fraud; Claim, false or fraudulent; Commercial bribery; Trust, abuse of.*

Personal checks, substituting for cash: An employee takes money from the cash register and substitutes a personal check. In that way, the cash drawer is always in balance, but the employee never submits the personal check for deposit to the company's bank account. Consequently, the employee receives free use of the cash.

Personal-injury insurance fraud: Report of a real but overstated physical injury or a false injury to an insurance company to recover unentitled benefits such as for a tort claim or reimbursement of fake medical expenses.

See also: *Casualty-insurance fraud; Insurance fraud.*

Personal property pawned: The perpetrator inflates the value of his or her personal belongings, insures them, and then pawns them for a lesser amount of cash. He or she then reports them stolen and files a claim. If the insurance payment is received, he or she then recovers the items from the pawnshop with a portion of the insurance payment and pockets the difference.

See also: *Insurance fraud; Property-insurance fraud.*

Pigeon drop or pocketbook drop: One of a large variety of street con games. The victim is persuaded to withdraw a large sum of cash from a bank account to show good faith or financial responsibility regarding the sharing of a "discovered" cache of money with two other persons (who are con artists). In the course of the con, both the "discovered" money and the victim's "good faith" money disappear as do the con artists.

Victims may be anyone, since perpetrators of this fraud have a remarkable ability through words to disarm their victims. Keys to the pigeon drop con are the following:

1. The con artists do not appear to be associated or know each other in any way.
2. A pocketbook, envelop, and so on, containing a sizable amount of money and no owner identification is "found" by one of the perpetrators who suggests the money is illicitly generated, for example, a gambler's proceeds.
3. The fraudsters agree to share the money with the victim who shows "good faith" to those involved by putting up money. Alternately, all may agree to put money into a pool to be held by a coconspirator, meaning, the one who did not find the money.
4. A switch is made while the victim is distracted, and his or her money is stolen by one of the perpetrators.

Pollution and environmental protection violation: One of many abuses that violates specific environmental- and pollution-control statutes and orders. White-collar crime abuses in this area consist primarily of the making or submitting of false statements concerning the degree of compliance with regulations for pollution control in order to cover up violations or lack of compliance with environmental standards. Falsification of test or sample data designed to measure compliance with standards represents another form of this violation.

See also: *Commercial crime; Environmental abuse; Statement, false.*

Ponzi scheme: This is a general class of fraud (a variation of the pyramid scheme) in which the fraudster uses money invested by later victims to pay a high rate of return to the first group of investors instead of making promised investments. These schemes must inevitably collapse because it is mathematically impossible to continue them indefinitely. The length of time they can continue will depend upon the promised rate of return to investors, the amount of money the fraudster takes out for him- or herself and the costs of inducing victims to part with their money (for example, sales commissions). Many of these frauds have cheated their victims of millions of dollars; some frauds have operated over a period of years.

Ponzi elements exist in many varieties of investment fraud under different guises and in different variations; for example, long-term investments and short-term business financing.

See also: *Investment fraud.*

Possession of property obtained by crime: An offense that refers either to the actual possession of property obtained by a crime or to the possession of proceeds from the disposal of property obtained by a crime.

See also: *Fraud.*

Price fixing: Illegal combinations by sellers to administer the price of a good or service, thus depriving customers of a competitive marketplace, restraining competition, and maintaining an artificial price structure.

Victims are customers who are deprived of freely determined prices for the goods and services they purchase. Secondary victims may be competitors of the firms participating in the price-fixing agreement.

See also: *Anti-trust offense; Trade, restraint of.*

Procurement fraud: Unlawful manipulation of the public or private contracting process to obtain an advantage.

Victims are competitors, the public or private entity soliciting bids it believes to be competitive as well as customers or constituents of those entities who do not realize the benefits that would be derived from a truly competitive procurement process.

Three main forms of competitive procurement fraud are the following.

1. *Bid rigging.* A form of illegal anticompetitive activity in which bidders in a competitive procurement collusively set their bids in such a way as to deprive the bid solicitor of a competitive process. The effect is an administered bidding process in which the winner and the terms and prices of the goods and services involved are set by the conspirators rather than by the competitive process. Parties to the conspiracy are thus able to divide

among themselves a set of procurement contracts and to fix prices for goods and services at the same time.

2. *Bid fixing.* A form of illegal manipulation of the procurement process whereby one bidding party is provided with inside information by the bid solicitor or an agent, which enables the said bidder to gain an unfair advantage over other bidders.

3. *Bribery and kickbacks.* The awarding of procurement contracts on the basis of the payment of bribes and kickbacks to procurement officials rather than on the basis of competitive procurement guidelines.

See also: *Claim, false or fraudulent; Commercial bribery; Kickback; Corruption, public or official.*

Product substitution: The substitution, without the knowledge of the purchaser, of a less expensive product or service. The purchaser is charged for the more expensive product or service and the fraudster pockets the difference.

See also: *Commercial crime; External fraud; Procurement fraud; Property-improvement fraud.*

Property-improvement fraud: The fraudster goes door-to-door promising repairs to property at bargain rates, collecting up-front money and then absconding with the proceeds. The victims are usually senior citizens.

See also: *External fraud.*

Property-insurance fraud: An insured reports a false theft, inflates the value of his or her personal belongings and pawns them or purposely destroys them to collect a benefit from the insurer.

See also: *Arson for profit; Insurance fraud; Personal property pawned; Repossessed household goods.*

Public or official corruption: See *Corruption, public or official.*

Purchases, unnecessary: Inventory ordered specifically for personal use, theft, or scrap proceeds. The embezzlements are then charged to inventory.

See also: *Acquisition and payment cycle; Inventory and warehousing cycle; Procurement fraud.*

Pyramid scheme: The commercial version of the chain letter scheme used by fraudsters to sell phony investments (Ponzi scheme), distributorships, franchises, and business opportunity plans.

See also: *Chain-referral scheme; Franchise fraud; Investment fraud.*

Real estate fraud: A form of loan fraud involving the purchase of under- or over-valued real estate.

See also: *External fraud; Loan or lending fraud; Mortgage security, false.*

Referral sales fraud: See *Chain-referral scheme; Merchandising fraud.*

Repair fraud: Consumer fraud involving repair or maintenance service performed on consumer goods.

These white-collar crime schemes generally involve the following:

1. Overcharging for services performed

2. Charging for services and parts not used
3. Performing services or repairs not wanted or needed
4. Failing to perform services or repairs promised

See also: *Consumer fraud.*

Reporting guidelines, breach of: A breach in defiance of a government requirement that banks assist in the prevention of money laundering by reporting details of large cash deposits. For example, a bank employee who conspires with a money launderer to make deposits without reporting the required details is breaching the reporting guidelines.

See also: *Money laundering*

Repossessed household goods: Household items are repossessed and the insured submits a false claim to the insurer reporting the property was stolen.

See also: *Insurance fraud; Property-insurance fraud.*

Repurchasing: A stock market manipulation in which the promoter buys back control of the company when the stock price reaches rock bottom.

See also: *Stock market manipulation.*

Risk factors, generic: Risk factors within the control of the entity protecting itself but outside the control of potential perpetrators.

Revenue recognition in the improper period: Preparation of false financial statements through the improper accruals of revenue on future, anticipated sales. Techniques include altering dates on shipping documents or holding the books open until after shipments have occurred. This technique is often used to inflate reported profits.

See also: *Financial statement, false; Revenue recognition on transactions that do not meet revenue recognition criteria.*

Revenue recognition on transactions that do not meet revenue recognition criteria: Preparation of false financial statements by improperly recognizing revenue on transactions for which the earning process is incomplete—for example, when the right of return exists, or on bill-and-hold transactions. The items involved are often concealed through the use of written side agreements or oral agreements that are not included with the company's books of account.

See also: *Financial statement, false; Revenue recognition in the improper period.*

Running a box: One or more persons control the movement of a stock to manipulate its price. They are called "the box."

See also: *Stock market manipulation.*

Sales and collection cycle: The billing of goods or services to customers, the setting up of accounts receivable for customers who purchase goods or services on credit and the collection of funds relating to those receivables.

Scrap, theft of: This kind of theft can be significant, especially if the thief has the authority to designate saleable inventory as scrap. In most companies, inventory scrap is easy to steal because it is not recorded or well controlled.

See also: *Procurement fraud.*

Secret commission: The most common form of procurement fraud. A secret payment is given, usually by a supplier to a purchasing agent, to buy the purchasing agent's influence on his or her employer's decision making.

See also: *Commercial crime; Kickback; Procurement fraud.*

Securities fraud: Fraudulent activities involving the sale, transfer, or purchase of securities or money interests in the business activities of others.

Victims are generally investors who are not aware of the full facts regarding transactions into which they enter. Abuses cover a broad range and can include, for example, the following situations.

1. Businesses or promoters seek to raise capital unlawfully or without proper registration and monitoring.
2. Securities of no value are sold or are misrepresented as being worth far more than their actual value.
3. Purchasers are not advised of all facts regarding securities and/or of the failure to file appropriate disclosures with federal and provincial regulatory agencies.
4. Insiders use special knowledge to trade in securities to the disadvantage of the general public.
5. Broker-dealers and investment advisers act for their own benefit rather than for the benefit of their clients.
6. False information is provided to security holders and the investing public in financial statements published or filed with securities regulatory agencies or in the media as a result of payments to financial writers or publications.
7. Manipulation of the price of securities by purchases and sales on the stock exchanges or over-the-counter markets.

Securities violations potentially exist wherever investors rely on others to manage and conduct the business in which an investment is made. It is not necessary that there be any formal certificates such as stocks and bonds. Any form of investment agreement is potentially a "security."

See also: *Advance-fee fraud; Boiler room; Insider trading; Investment fraud; Statement, false.*

Self-improvement scheme: This kind of fraud appeals to the victim's desire to improve him- or herself personally or financially by the acquisition of social, employment, or physical skills or attributes.

Schemes in this category tend to run on a continuum from improving purely personal or social skills and attributes to those tied to an individual's employment opportunities. On the personal end of the scale are the dance studio or charm school schemes; on the employment end of the scale are fraudulent job training schemes and advance fee employment agencies.

Somewhere in the middle are modeling agencies which purport to both improve the "person" and his or her employment prospects. Also included are courses on improving one's image or ability to communicate with others. Some business opportunity schemes, which hold out the prospect of financial improvement plus "being a respected community businessperson," also fall into this category by appealing to the victim's desire to improve his or her finances and lifestyle.

See also: *Business-opportunity fraud; Employment-agency fraud; Vanity-publishing scheme.*

"Sewer" service: A term used to describe the kinds of activity noted below.

Many merchandising, home repair, and other kinds of fraud rely on the use of litigation for ultimate collection of the proceeds of the fraud. Likewise, many enterprises that are not strictly speaking fraudulent, for example, those that sell much overpriced merchandise on credit, also depend on litigation or the threat of litigation to squeeze money from victims.

In both these situations, devices are often adopted to fraudulently deprive victims of the opportunity to defend against litigation–usually by not informing them that litigation has been initiated against them (that is, dropping the summons or subpoena "down the sewer"). This is accomplished, usually, by false affidavits, filed in court, that a summons and complaint were served on the victim.

See also: *Stock market manipulation.*

Sham, corporate: The use of a corporate entity to provide a veil of respectability and substance for fraudulent activity.

See also: *Commercial crime.*

Sham transaction: A fraudulent transaction giving the impression of a legitimate transaction at a higher price. These transactions are particularly difficult to detect because they involve collusion with a co-conspirator outside the entity.

See also: *Sham, corporate.*

Shell company: An inactive company whose shares have been repurchased.

Short weighting or loading: Deliberate shorting of the volume or quantity of a cargo or other purchase. The short load is accompanied by a false invoice demanding payment for the full amount. This kind of fraud is easiest to perpetrate where the goods involved are of a nature or bulk that it is difficult for the receiver to detect shortages.

The reverse of the short weighting or loading fraud is often used as a modus operandi for theft of cargo. In this situation, a transport vehicle is intentionally overloaded; the overage is not recorded and the overloaded amount forms the basis of kickbacks to the scheme operators from the recipient of the shipment, who is often the fence for the stolen goods. Manipulation of the size or volume of loads must always be accompanied by false documentation.

This violation involves either a false claim to a customer or a plain and simple theft from the shipper. Because insiders are frequently involved, it will often involve commercial bribery, kickbacks, and so on.

See also: *Weights and measures fraud.*

Short selling: A technique whereby the trader is gambling that the price of a stock will fall. Thus, he or she anticipates a profit on the transaction by selling a number of shares first, for later delivery at a specified price. The trader then buys those shares at a later date, when, if his or her gamble were correct, the share price has fallen and he or she delivers them. Thus, the trader makes a profit during a period of declining prices of the stock.

Siphoning funds: Illegal withdrawal of money in small amounts from a large number of accounts. For example, pennies and portions of pennies (resulting from rounding off) can be shaved from thousands of savings accounts. The money is then accumulated in a single account that is accessed by the embezzler.

Skimming: A scheme in which cash is skimmed before it enters the accounting system. For example, an employee accepts cash but never prepares a receipt or prepares a receipt for less than the amount received.

See also: *Sales and collection cycle.*

Smurfing: The use of couriers (also known as *smurfs*) to deposit and withdraw cash or cash equivalents at financial institutions in amounts less than the reporting limit to avoid reporting requirements.

See also: *Money laundering.*

Statement, false: The concealment or misrepresentation of a fact material to the decision-making process of an entity. The false statement is often the means by which a fraudulent scheme to obtain money or benefit is effected for either of the following, among other, reasons.

1. The false statement constitutes the underlying documentation for a false claim.
2. The false statement impedes discovery of the fraudulent scheme, that is, covers up the fraud. These statements often provide the opportunity for conditioning the victim to unquestioningly accept and approve a false claim.

See also: *Claim, false or fraudulent; Ghost employee; Government-benefit program, fraud against.*

Stock market manipulation: A crime perpetrated by a stock promoter who artificially influences the market price of shares in a company for personal gain at the expense of the investing public.

See also: *Commercial crime; Securities fraud.*

Street certificate: A stock certificate that has been issued in the name of a brokerage firm and then endorsed by it. It is now like a bearer certificate and can change hands several times in many trades without being returned to a trust company for transfer.

Taking out the market: See *Cleaning up the market.*

Talent-agency scheme: See: *Self-improvement scheme; Vanity-publishing scheme.*

Tax and revenue violation: Fraud perpetrated with the intent to deprive a taxing authority of revenue to which it is entitled or of information it needs to make a judgment regarding revenues to which it is entitled or to avoid admission of involvement in illicit, though profitable, business activities.

Tax fraud may be perpetrated through the filing of a false return, as in personal income tax fraud; through the bribery of a public official, as may occur in property tax assessment fraud; or in the failure to file appropriately, as with an organized crime-figure who may not be concerned with avoiding tax liability but rather with revealing the sources of his or her taxable income. Many white-collar crimes obligate the offender to commit tax fraud because of illicitly obtained money he or she does not wish to report, for example, assets due to bribe, larceny, kickback, or embezzlement proceeds. Common crimes, especially of a business nature, also result in tax violations, for example, bookmaking and fencing stolen goods, which could be income and sales tax abuses.

Tax avoidance through false statements may be a component of otherwise legitimate business enterprises, especially in the areas of business and occupation taxes, inventory taxes, and sales taxes. Individuals and businesses will also seek to avoid or evade excise taxes, for example, on cigarettes or in the case of tanker trucks by the substitution of low-taxed home heating oil for higher-taxed diesel fuel.

See also: *Income tax fraud.*

Trade, restraint of: Actions, combinations, or schemes that interfere with unfettered marketplace transactions. Examples are price fixing, bribery and kickbacks for commercial advantage, interference with competitive bidding processes, dictation of price structure to customers or dealers, and exclusive buying arrangements.

See also: *Commercial bribery; Price fixing; Procurement fraud.*

Transactions, entering false: Entering invoices for fake vendors into the accounts payable system or recording false credit memos to reduce legitimate accounts receivable.

See also: *Acquisition and payment cycle; Sales and collection cycle.*

Trust, abuse of: Misuse of one's position and/or privileged information gained by virtue of that position to acquire money, property, or some privilege to which one is not entitled. Abuse of trust also often involves a violation of fiduciary duty.

Abuse of trust can occur in many areas but arises most frequently in the following four white-collar crime areas.

1. *Banking*: Self-dealing in connection with loans or credit to oneself, one's friends, or business associates.
2. *Securities.* Insider information used for personal benefit at the expense of clients, stockholders, and others.
3. *Commercial bribery.* Manipulation of procurement and competitive bidding processes.
4. *Embezzlement.* Misuse of property or funds in the custody of a trustee.

See also: *Banking fraud; Commercial bribery; Embezzlement and fiduciary fraud; Insider trading; Procurement fraud; Securities fraud.*

Trust fund, misappropriation of: The diversion of client funds held in trust and use of the money for purposes other than those intended by the client.

See also: *External fraud.*

Vanity-publishing scheme: Any scheme that involves eliciting fees from individuals on the promise of promoting their creative "talents" (real or imaginary) or assisting them in the development of said "talent."

The success of these kinds of fraud relies on the victim's vanity about his or her hitherto unrecognized talent. These schemes work best in areas such as literary publishing or song writing, where taste is more important than performance standards.

The fraudster will imply a promise of national advertising, book reviews, distribution, and special marketing services but not so concretely that he or she will be held to any obligation. The victims usually invest heavily and lose both their money and their hopes. They are left with a few copies of a printed and scored song arrangement or a number of copies of books that established book review publications have not troubled to look at because of their publishing source.

See also: *Self-improvement scheme.*

Warehousing: Part of a stock market manipulation that places shares into the hands of people who are friendly to the promoter—warehousing or parking—to allow the promoter to maintain control of the shares and continue to restrict and regulate their availability.

Wash-trading: A flurry of trading activity falsely created by the promoter's group to give the appearance of great interest in the stock to increase demand for the stock among the public to whom the promoter plans to eventually sell his holdings when the price reaches a certain level.

See also: *Stock market manipulation.*

Weights and measures fraud: Cheating customers by failure to deliver prescribed weights or volumes of desired goods. The victim is defrauded by relying on the false documents provided by the fraudster testifying to the delivered quantities.

Examples of white-collar crimes include the following:

1. Gas pump meter manipulation to show more gas pumped than received by the customer
2. Odometer rollbacks in auto sales

These kinds of fraud are most successful if the victim cannot easily verify the accuracy of the measuring devices or if the victim has no reason to question the seller's claim or statement, for example, when the products sold are bottled or packaged.

See also: *Short weighting or loading.*

Welfare fraud: Abuses of government income and family subsidy programs.

Government welfare programs are often exploited by applicants who apply for benefits to which they are not entitled or continue to claim eligibility even though they no longer meet the eligibility criteria.

Receipt of money from claimants by officials processing welfare claims represents another dimension of this fraud. These monies may be solicited as kickbacks in exchange for the filing of inflated claims; as bribes to certify claimants who are ineligible or to avoid reporting claimants' ineligibility or as extortion for processing claims to which a recipient is fully eligible. In some cases, nonexistent recipients (*ghosts*) may be created to fraudulently siphon money out of the programs.

See also: *Government-benefit program, fraud against.*

White-collar crime: Nonviolent crime for financial gain committed through deception by entrepreneurs, professionals, or semiprofessionals using their special occupational skills and opportunities. This category also includes similar crimes committed by anyone having special technical and professional knowledge of business and government, irrespective of the person's occupation.

See also: *Commercial crime; Economic crime.*

Work-at-home schemes: See *Business-opportunity fraud; Franchise fraud.*

Written-off account, diversion of payments from: Diversion of payments received from a customer whose account has been written off. Because most companies do not monitor defunct accounts, this activity is rarely detected. For example, an employee will work with a customer to collect an overdue receivable. Before the customer pays, the employee writes off the account, removes it from the books, and pockets the funds received.

See also: *Internal fraud; Sales and collection cycle.*

BIBLIOGRAPHY

Set out below is a selected list of books and Web sites for further reading on the subject of fraud, commercial crime, and related topics.

BOOKS

Albanese, Jay S. *White-Collar Crime in America.* Englewood Cliffs, NJ: Prentice Hall, 1995.

Beasley, Mark S., Joseph V. Carcello, and Dana R. Hermanson. *Fraudulent Financial Reporting 1987-1997: An Analysis of U.S. Public Companies.* New York: Committee of Sponsoring Organizations of the Treadway Commission, 1999.

Beaven, Guy W. *Hello Suckers!: Inside the Brutal World of Stock Market Scams and How to Prevent Falling Victim.* Washington Grove, MD: Gordon-Richardson Press, 1995.

Bequai, August. *White Collar Crime: A Twentieth Century Crisis.* Lexington, MA: D.C. Heath, 1978.

Bertrand, Marsha. *Fraud!: How to Protect Yourself from Schemes, Scams, and Swindles.* New York: American Management, 1999.

Binstein, Michael, and Charles Bowden. *Trust Me: Charles Keating and the Missing Billions.* New York: Random House, 1993.

Bintliff, Russell L. *Complete Manual of White Collar Crime Detection and Prevention.* Englewood Cliffs, NJ: Prentice Hall, 1993.

Black, Henry C. *Black's Law Dictionary: Fifth Edition.* St. Paul, MN: West Publishing, 1979.

Bologna, Jack, and Paul Shaw. *Avoiding Cyber Fraud in Small Businesses.* New York: John Wiley & Sons, 2000.

______. *Corporate Crime Investigation.* Boston: Butterworth-Heinemann, 1997.

Bologna, Jack. *Handbook on Corporate Fraud: Prevention, Detection, and Investigation.* Boston: Butterworth-Heinemann, 1993.

Brickey, Kathleen F. *Corporate and White Collar Crime: Selected Cases and Statutes.* New York: Aspen Law & Business, 1997.

Bucy, Pamela H. *White Collar Crime: Cases and Materials.* St. Paul, MN: West Group, 1998.

Calavita, Kitty, Henry N. Pontell, and Robert H. Tillman. *Big Money Crime: Fraud and Politics in the Savings and Loan Crisis.* Berkley: University of California Press, 1997.

Camerer, L. *Costly Crimes, Commercial Crime and Corruption in South Africa.* Johannesburg: Institute for Security Studies, 1997.

Cole, Richard B. *Management of Internal Business Investigations: A Survival Guide.* Springfield, IL: Charles C. Thomas, 1996.

Coleman, James William. *The Criminal Elite: Understanding White-Collar Crime.* New York: St. Martin's Press, 1998.

Comer, Michael J. *Corporate Fraud,* Second Edition. New York: McGraw-Hill, 1998.

______, Patrick M. Ardis, and David H. Price. *Bad Lies in Business: The Commonsense Guide to Detecting Deceit in Negotiations, Interviews, and Investigations.* New York: McGraw-Hill, 1992.

Croft, Roger. *Swindle!: A Decade of Canadian Stock Frauds.* Toronto: Gage Pub., 1975.

Dailey, Edward J. *Health Care Fraud: A New White Collar Crime: Strategies for Compliance, Audit, Litigation, and Prosecution.* Boston: MCLE, 1997.

Durkin, Ronald L., and Everett P. Harry III. *Fraud Investigations in Litigation and Dispute Resolution Services: A Nonauthoritative Guide.* New York: American Institute of Certified Public Accountants, Inc., 1997.

Dykeman, Francis C. *Forensic Accounting: The Accountant as Expert Witness.* New York: John Wiley & Sons, 1982.

Edelhertz, Herbert, James O. Golden, and Stephen W. Cooley. *The Investigation of White-Collar Crime: A Manual for Law Enforcement Agencies.* Washington, DC: U.S. Dept. of Justice, 1977.

Elliott, Robert K., and John J. Willingham. *Management Fraud: Detection and Deterrence.* New York: Petrocelli Books, 1980.

Frank, Peter B., and Michael J. Wagner. *Providing Litigation Services.* New York: American Institute of Certified Public Accountants, 1993.

Garman, Thomas E. *Ripoffs and Frauds, How to Avoid and How to Get Away.* Houston: Dame Publications, 1996.

Geis, Gilbert, Robert F. Meier, and Lawrence M. Salinger. *White-Collar Crime: Classic and Contempory Views.* New York: Free Press: Distributed by Simon & Schuster, 1995.

Ghosh, Anup K. *E-Commerce Security: Weak Links, Best Defenses.* New York: John Wiley and Sons, 1998.

Grau, J. J., and B. Jacobson. *Criminal and Civil Investigation Handbook.* New York: McGraw-Hill, 1993.

Green, Gary. *Occupational Crime.* Chicago, IL: Nelson-Hall, 1997.

Haynes, Stephen L. *Computers and Litigation Support.* New York: Harcourt Brace Jovanovich, 1981.

Hogue, Elizabeth E., Sanford V. Teplitzky, and Howard L. Sollins. *Preventing Fraud and Abuse: A Guide For Medicare and Medicaid Providers.* Owings Mills, MD: National Health Pub., 1988.

Hoyt, Douglas et al. *Computer Security Handbook,* Second Edition. New York: MacMillan Publishing Company, 1995.

Janal, Daniel S. *Risky Business : Protect Your Business from Being Stalked, Conned, or Blackmailed on the Web.* New York: Wiley, 1998.

Judson, Karen. *Computer Crime: Phreaks, Spies and Salami Slicers.* Berkley Heights, NJ: Enslow Publishers, 1999.

Katz, Leo. *Ill-Gotten Gains: Evasion, Blackmail, Fraud, and Kindred Puzzles of the Law.* Chicago: University of Chicago Press, 1996.

Kirk, Paul L., and John I. Thornton, Eds. *Crime Investigation,* Second Edition. New York: John Wiley & Sons, 1985.

Krauss, Leonard I., and Aileen MacGahan. *Computer Fraud and Countermeasures.* Englewood Cliffs, NJ: Prentice-Hall, 1979.

Langdale, Rachel. *Case Studies in Corporate Crime.* Sydney: NSW Bureau of Crime Statistics and Research, 1990.

Leonard, Orland. *Corporate and White Collar Crime: An Anthology.* Cincinnati, OH: Anderson Publishing, 1995.

Levi, Michael. *Fraud: Organization, Motivation, and Control.* Aldershot, England; Brookfield, VT: Ashgate, 1999.

Magnuson, Roger J. *The White Collar Crime Explosion: How to Protect Yourself and Your Company from Prosecution.* Minneapolis, MN: Dorsey & Whitney, 1992.

Manning, George A. *Financial Investigation and Forensic Accounting.* Boca Raton, FL: CRC Press, 1999.

Mazer, Robert E., and S. Craig Holden. *Medicare Anti-Fraud and Abuse: A Guide For Hospitals, Labs & MDs.* Washington, DC: Washington G-2 Reports, 1992.

McMahon, David. *Cyber Threat.* Toronto: Warwick Publishing, 2000.

Moscarino, George J., and Charles M. Kennedy. *Corporate Investigations: A Practical Primer.* Washington, DC: Washington Legal Foundation, 1996.

National Association of Certified Fraud Examiners. *Cooking the Books: What Every Accountant Should Know About Fraud.* New York: NASBA, 1993.

Neilson, R. Todd, et al. *Providing Bankruptcy and Reorganization Services: A Nonauthoritative Guide.* New York: American Institute of Certified Public Accountants, 1998.

Nelken, David. *White-Collar Crime.* Aldershot, Hants, England; Brookfield, VT: Dartmouth Publishing, 1994.

Nossen, Richard A. *The Detection, Investigation, and Prosecution of Financial Crimes.* Richmond, VA: Thoth Books, 1993.

Parker, Donn B. *Fighting Computer Crime: A New Framework for Protecting Information.* New York: Wiley Computer Publishing, 1998.

Pipkin, Donald L. *Information Security: Protecting the Global Enterprise.* Upper Saddle River, NJ: Prentice Hall PTR, 2000.

Podgor, Ellen S., and Jerold H. Israel. *White Collar Crime in A Nutshell.* St. Paul, MN: West Publishing, 1997.

Poveda, Tony G. *Rethinking White-Collar Crime.* Westport, CT: Praeger, 1994.

Rae, Weston. *Combating Commercial Crime.* North Ryde, NSW: Law Book, 1987.

Ramachandran, K.S. (Kattalai Sivasubramanya). *Scanning the Scam: How and Why of the Securities Scandal.* New Delhi: Neo Publishing, 1993.

Ramos, Michael J., and Anita M. Lyons. *Considering Fraud in a Financial Statement Audit: Practical Guidance for Applying SAS No. 82.* New York: American Institute of Certified Public Accountants, 1997.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World.* New York: John Wiley and Sons, 2000.

Siegel, Larry J. *Criminology: Theories, Patterns and Typologies, Third Edition.* St. Paul, MN: West Publishing Company, 1992.

Soble, Ronald L., and Robert E. Dallos. *The Impossible Dream: The Equity Funding Story, the Fraud of the Century.* New York: New American Library, 1975.

Stephenson, Peter. *Investigating Computer-Related Crime: Handbook for Corporate Investigators.* Boca Raton, FL: CRC Press, 1999.

Tomes, Jonathan P. *Fraud, Waste, Abuse and Safe Harbors: A Guide for the Healthcare Professional.* Chicago: Probus Publishing, 1993.

______. *Healthcare Fraud, Waste, Abuse, and Safe Harbors: The Complete Legal Guide.* Chicago: Probus Publishing, 1993.

United States Congress. *Federal Efforts to Combat Fraud, Abuse, and Misconduct in the Nation's S & L's and Banks.* Washington, DC: U.S. G.P.O., 1990.

Wagner, Charles R. *The CPA and Computer Fraud.* Lexington, MA: Lexington Books, 1979.

Wadlow, Thomas A. *The Process of Network Security: Designing and Managing a Safe Network.* Reading, MA: Addison Wesley Longman, 2000.

Walter, Ingo. *The Secret Money Market: Inside the Dark World of Tax Evasion, Financial Fraud, Insider Trading, Money Laundering, and Capital Flight.* New York: Harper & Row, Ballinger Division, 1990.

Wellman, Francis L. *The Art of Cross-Examination.* New York: Dorset Press, 1997.

Wells, Joseph T. *Occupational Fraud and Abuse.* Austin, TX: Association of Certified Fraud Examiners, 1997.

Wells, Joseph T., et al. *Fraud Examiners Manual, Third Edition.* Austin, TX: Association of Certified Fraud Examiners, 1998.

Williams, Howard E. *Investigating White-Collar Crime: Embezzlement and Financial Fraud.* Springfield, IL: C.C. Thomas, 1997.

WEB SITES

Advance Fee Frauds: Nigerian Scams. http://home.rica.net/alphae/419coal/

The Association of Certified Fraud Examiners. http://www.cfenet.com

Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees, 1999. http://www.nyse.com/ and http://www.nasdaqnews.com/.

The Committee of Sponsoring Organizations of the Treadway Commission. http://www.coso.org/main.htm

CSCAP Working Group on Transnational Crime. http://www.cscap.org/crime.htm

Fighting Fraud and Corruption. http://www.ex.acuk/~RDavies/arian/scandals/fight.html

Fraud Bureau. http://www.fraudbureau.com

Fraud Defense Network. http://www.frauddefense.com

Fraud Internet Information. http://dir.yahoo.com/Computers_and_Internet/Internet/Business_and_Economics/Fraud/

Fraud on the Internet Resource List. http://www.emich.edu/public/coe/nice/fraudrl.html

Fraudnet. http://www.auditnet.org/fraudnet.htm

Fraud News. http://www.fraudnews.com

The Institute of Internal Auditors. "Struggling to incorporate the COSO recommendations into your audit process? Here's one audit shop's winning strategy." Dennis Applegate and Ted Wills. December 1999. http://www.coso.org/Articles/audit_shop.htm.

International Association of Financial Crimes Investigators. http://www.iafci.org/start.html

National Check Fraud Center. http://www.ckfraud.org

National Fraud Information Center. http://www.fraud.org

Securities and Exchange Commission. Internet Fraud: How to Avoid Internet Investment Scams. http://www.sec.gov/consumer/cyberfr.htm

Securities and Exchange Commission. "The Numbers Game", a speech presented to the New York University Center for Law and Business by Arthur Levitt, Sept. 28, 1998. http://www.sec.gov/news/speeches/spch220.txt.

White-Collar Crime: Loss Prevention Through Internal Control. Prepared for Chubb Group of Insurance Companies by Ernst & Young. http://www.chubb.com/library/wcrime.html

Report on Fraud

REPORT ON

Fraud

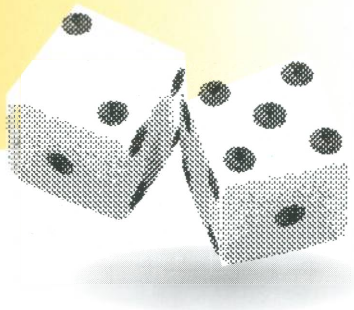
Volume 2 . Issue 4 . January 2000

Kroll Lindquist Avey
FORENSIC ACCOUNTING, LITIGATION CONSULTING, BUSINESS VALUATION

The Canadian Institute of Chartered Accountants

AICPA
American Institute of Certified Public Accountants

Leaving [for] Las Vegas



Looking for a fraudster on the lam? Take a gamble on Las Vegas. The odds are good you'll find him there.

IT SEEMS ONLY FITTING that the city founded by mobster Bugsy Siegel in the 1940s has become the destination of choice for felons fleeing the law. Las Vegas is America's fastest growing metropolitan area, with a population of 1.3 million. It also welcomes about a half million people a week, making it a seemingly ideal place to become lost in the crowd.

"Sooner or later they all end up in Vegas," Alfredo Cervantes, a sergeant with the Las Vegas Criminal Apprehension Team, told the *Los Angeles Times.* "Criminals, like everybody else, know they can get anything and everything here, from girls to gambling. If they do get caught, at least they had one last hurrah in Sin City."

And many of them do get caught, at a higher rate than anywhere else in the U.S. "During the first 10 months of fiscal year 1999, the Las Vegas task force arrested 840 felons, the largest number by any of the 56 fugitive U.S. apprehension teams," reported the *Times.* "In the same period, the Los Angeles team netted 382 arrests, New York's 301 and San Francisco's 251."

Among the apprehended fraudsters was a disgraced New Jersey prosecutor who skipped bail after being arrested on corruption and tax fraud charges. During his time in Las Vegas he may have taken in a strip show performed by a New York drug dealer. She was arrested onstage when task force officers noticed her tell-tale snake tattoos.

One of the more unusual arrests occurred last September, soon after a restaurant cashier finished a *Reader's Digest* article about Grant Warren Beaucage, who was wanted in Canada for the murder of his wife. The cashier put down the magazine and looked up at the man about to pay for his meal. She recognized him as Beaucage, from the picture in the article, and alerted hotel security. He was apprehended a short time later.

Considering that fraudsters often have a large stash of money with them, it seems likely that Vegas' bright lights would be a particularly compelling lure for them. And it might turn out to be a smart place to hide. "Sorting through 700 warrants each month, [the Criminal Apprehension Team] forsake embezzlers and scam artists for the more violent elusive offenders," reported the *Times.* But even if fraudsters do gain freedom in Las Vegas, we can take some solace in assuming that most of them will lose their ill-gotten gains in the casinos.

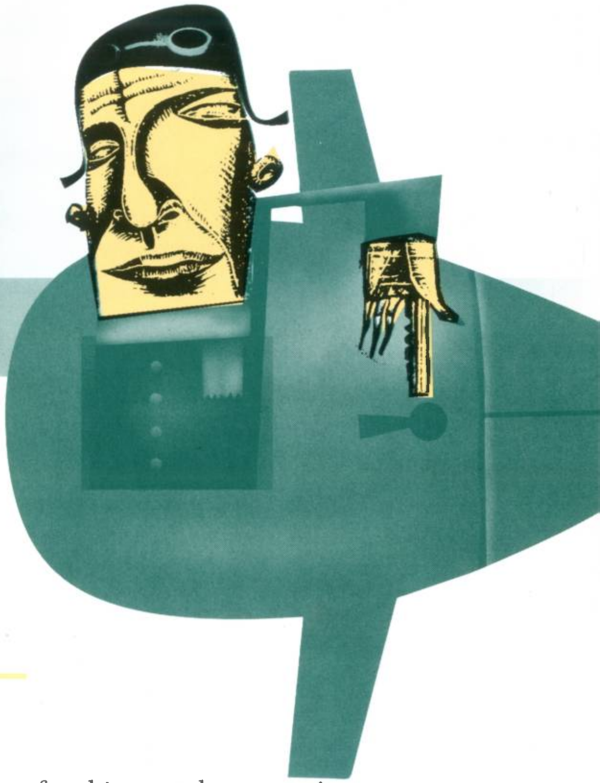
– Paul McLaughlin, editor

REPORT ON **Fraud**

Subscription/Order Enquiries
In Canada
Toronto calling area: (416) 977-0748
Rest of Canada: 1-800-268-3793
Facsimile: (416) 204-3416
On the net: www.cica.ca/Order
In the United States
Phone: (888) 777-7077
Facsimile: (800) 362-5066
Email: memsat@aicpa.org
(ask for *CPA's Handbook of Fraud and Commercial Crime Prevention,* PC #056504NL)

Report on Fraud is published six times annually by The Canadian Institute of Chartered Accountants, Kroll Lindquist Avey, and the AICPA. Copyright © 1998
In Canada
Annual subscription $125.00
7% GST/HST applies to all domestic copies, GST/HST registration number R106861578, Quebec residents add GST plus 7.5% QST, QST registration number R1010544323 TQ 0001 SS.
In the United States
Report on Fraud is available to purchasers of the *CPA's Handbook of Fraud and Commercial Crime Prevention.*

Giving Fraud the *Finger*



Think only criminals have their fingerprints taken? Then you don't know about biometrics security. You likely soon will.

PIN NUMBERS and other types of security codes, passwords and cards for banking and other financial transactions will likely become obsolete in the next few years. "As we know, these systems offer a limited level of security from fraud," says Dr. Edward Cheng, VP of Public Relations with SecuGen Corporation, a global biometrics company located in Silicon Valley, CA. "But a fingerprint is unique to each person. Even identical twins have different fingerprints. So a fingerprint cannot be stolen or copied."

Biometrics is the automated method of using an individual's distinct biological features for security purposes. This technique can verify an individual's identity using physical measurements such as fingerprints, palm size, facial features, iris scans and voice recognition.

SecuGen has recently begun a pilot project with ING Direct, Canada using a fingerprint biometrics security system for ING's Internet banking products. ING Direct is a member of the ING Group, one of the world's largest financial institutions, with assets exceeding US$430 billion. Under the project, about 500 of ING's customers will use a special mouse developed by SecuGen, known as EyeD Mouse II, that has built-in fingerprint recognition technology.

The users must first register their thumbprint with ING (a one-time enrollment done over the Internet). When they log on to conduct a banking transaction, for example, their thumbprint is scanned by their mouse (there is a small glass section on the left side of the mouse, known as a platen, where the thumb of the right hand typically rests) to confirm their identity. The verification takes less than a second.

"We're already using this type of system with other companies, for things such as security access to offices," says Dr. Cheng. "But this project, I believe is the first ever with a financial institution." He says the system is highly accurate, which was not necessarily the case with earlier versions of this technology. "A person's unique features are extracted and turned into a 60-digit code number," he says. "The image is basically distortion-free."

Less worrisome than the quality of the technology is the question about consumer response to having their fingerprints stored in the computers of a large corporation. "The fear of 'Big Brother' is certainly a concern with some people," says Dr. Cheng. "But we've found that once they understand how secure their fingerprints are from misuse, they are very happy to cooperate with a system that protects them from fraud." ■

ILLUSTRATION BY JOSH LEIPCIGER

Getting *Soft* On Fraud

by Jock Ferguson

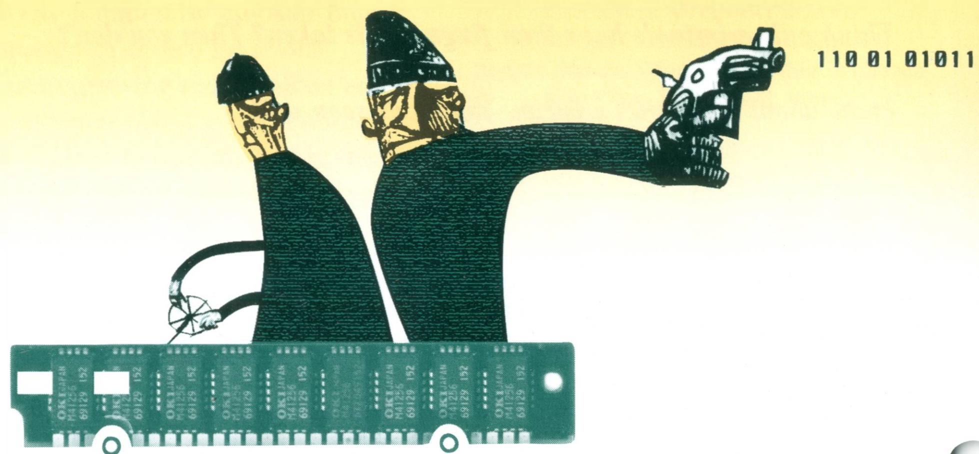


ILLUSTRATION BY JOSH LEIPCIGER

Fraud detection goes high-tech as many industries turn to software programs to uncover scams.

THE 3-D COMPUTER graphic swirled around and revealed a tall tower with many strings attached. It was a graphic representation of a high-rise building on Toronto's Yonge Street and the strings represented 167 people from that address who had filed insurance claims with a prominent Canadian insurance company.

The next graphic showed that 130 people from a two-story building outside Ottawa had all made claims with the same insurer.

With a look of horror, an executive from the insurance firm scribbled down the addresses as he suddenly realized both buildings were office towers – not residential locations, as the claims indicated. It was a telltale sign the claims were suspect.

In the very recent past those fraudulent claims might not have been uncovered. They would likely have contributed to the $1.3 billion insurance losses a year, which makes insurance fraud one of Canada's biggest white-collar crime problems. But they were detected, during an impressive demonstration of a new software program called "Fraud Investigator" from InfoGlide Corp.

Fraud Investigator was run on the insurance company's computer database. In a matter of minutes, the software found serious problems that the insurance company's existing fraud detection methods had not discovered.

"We searched claims and residential addresses and then had the program visualize the

addresses with the most claimants," says Lee Thistle of TSI Solutions Inc., the Canadian distributor of Fraud Investigator.

Most insurance computer systems in Canada have little or no ability to search their own databases to find suspect claims. But the patented "similarity search engine" at the heart of Fraud Investigator can detect any possible interrelated data in insurance claims.

Fraud-detecting software is a recently new tool on the marketplace. It's of value to most sectors that face large-scale fraud, but particularly the insurance industry, banks, telephone companies and government health insurance plans.

One Size Doesn't Fit All

Report on Fraud set out to discover what software was on the market and how companies and professionals can best judge what will work for them. We quickly discovered there is no "one size fits all" solution.

Insurance industry chatter is focused on Fraud Investigator because it was the clear winner of an informal fraud detection software test run by the U.S. National Insurance Crime Bureau (NICB). (See sidebar on page 7.)

Fraud Investigator's similarity search engine can cross-search multiple databases even if they have different formats and "dirty data" containing numerous errors. It can find names, addresses and as many as 30 other identifiers, even if criminals have carefully changed the data to avoid detection. As well, it can incorporate other public records to expand its own detection effectiveness.

Scott Bothwell of the NICB says it plans to use the Internet so that insurance companies using Fraud Investigator can access NICB's questionable claims database to check to see if a person, or someone similar to that person, has filed multiple claims with different companies. This would allow them to conduct a search in real time and approve or reject a claim very quickly.

Another characteristic that makes Fraud Investigator popular is its ease of use. Field investigators need only a day's training and do not require the assistance of computer programmers.

InfoGlide is initially marketing the software to the property and casualty segment of the insurance industry, but will soon target auto and healthcare insurers. It says the similarity search technology is also being used by a U.S. intelligence agency to help track terrorists.

Fraud Investigator may also prove effective in combating some forms of Internet fraud. InfoGlide just signed a contract with the leading Internet auction site, eBay Inc., to help it attack identity fraud. The problem of customers who take money from purchasers and then never deliver the goods has plagued eBay. It will use InfoGlide software to keep known fraudsters off its network even if they change their names and other identifiers. In a test on eBay's computer system, the InfoGlide software found one person posing as 345 others, the company says.

Tracking Telephone Fraud

A very different type of software is being used to combat fraud in the telephone industry. Most phone companies use a form of neural network technology that tracks customer calling-patterns and flags any unusual deviations.

An explosion of wireless and Internet services has made the telecom industry more prone to fraud than ever. An estimated $6–$8 billion a year is siphoned from telephone revenue in the U.S. Typical frauds include:

...continued

- *cloning cell phones* – duplicating transmitter codes of individual phones and then using the code to run up huge long distance charges that are billed to the unsuspecting cell phone owner. It's a favorite trick of Canadian telemarketing fraudsters who target Americans
- *dial-through fraud* – hacking into corporate PBX systems and then making long distance calls
- *calling card theft* – stealing calling card numbers and selling them on the black market
- *clip-on fraud* – tapping into an exposed telephone line outside an office building and then selling access to unlimited numbers of people. It's prominent in poor ethnic communities where many people lack the means to make telephone calls home.

MCI Worldcom's "Sheriff" program and "Supersleuth" from Nortel Networks are leading solutions in the telecom industry.

Nortel developed its anti-fraud software over the past decade in its UK labs and commercialized it two years ago. It's based on neural network artificial intelligence technology that is modeled on human thought patterns, says Walt Shedd, Nortel's vice president of business development for North America.

Supersleuth has been a hot seller with German, Dutch and Central American cell phone firms. As well, four local exchange carriers in the U.S. are using it, as are two Canadian companies.

The rise of flexible, unified voice, data and Internet networks has increased the vulnerability to fraud. There are about 50 different forms of fraud, including subscription fraud, identity fraud, technical cloning fraud in analog wireless networks and clip-on fraud in landline networks.

"We see different types of fraud emerge almost on a daily basis and a lot of times it may be just a variation of an old scheme," Shedd says. "It takes awhile for people to see it."

> *"Computers are useless. They can only give you answers."*
>
> *– Pablo Picasso*

With Supersleuth, he adds, "we're looking at 70 different events or characteristics in any given record and mapping that to known fraud types. We're also looking at what is expected behavior within this service being provided and we're tracking deviations from that behavior. We've found that 100 per cent of the time if a new fraud is perpetrated it may not show up and be recognizable as something we've seen in the past. But it certainly will show up as something that is not expected."

Supersleuth can work with any type of computer network. It reaches into a database and collects records, analyzes them and produces results so an analyst can see if it's a high priority alarm.

An independent study of 40 global wireless operators, each with its own anti-fraud program, showed they averaged one fraud analyst per 133,000 subscribers. Those using Supersleuth averaged one analyst for every 666,000 subscribers, making the phone company's "hair and blood" costs substantially lower, Shedd says.

As well, the hardware costs associated with installing Supersleuth were one-quarter to one-half the cost of competitive systems. Pricing for the software is based on the size of a company's subscriber base, typically being less for smaller companies and more for larger.

Benefit to Banks

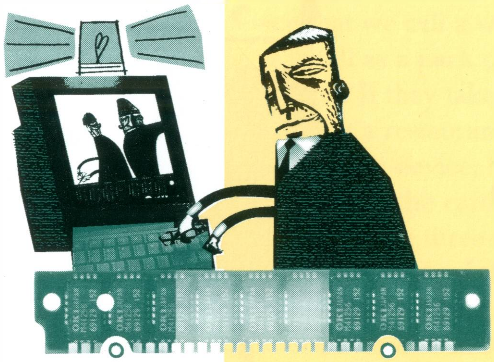
Banks are a prime target of fraudsters. Stolen credit and debit cards (see "*Card Tricks*," page 8) are a multi-billion dollar a year problem for banks and the outsourcing industry that banks use to process credit and debit card transactions.

As with telephone companies, banks use neural networking software to scan transaction patterns and recognize any deviations from established customer practices. For instance, if a credit card is used normally in a certain geographic area, say Quebec, and then suddenly is used in Mexico, the software will flag the transaction. A bank analyst may then decide to require an identification check of the cardholder before the bank will approve further charges.

International Neural Machines Inc. (INM) of Waterloo, ON has developed anti-fraud software for Canadian and Mexican banks. The data mining software searches the bank's databases and analyzes transactions, comparing them to the past history of customers and merchants to recognize potentially fraudulent activity. Its software has the advantage of learning from the data it searches to pick up new tactics that criminals may develop, says Oleg Feldgajer, president of INM. The company recently received a contract from the World Bank to install its hybrid software in the Central Bank of Estonia specifically to combat money laundering in the country's small banking sector.

INM is also in discussions with Canada's new anti-money laundering agency, FINTRAC, to provide it with software to help monitor cross-border financial transactions including inter-bank wire transfers to detect money laundering. In time, the scrutiny will be run via the Internet, making laundering analysis much faster and more effective. ■

Jock Ferguson is a Toronto writer.



Softness Tests

How do you decide which software is best for your needs? Put them to the test.

OBVIOUSLY you can hire a consultant to advise you of your needs, but at the end of the day there is only one reliable method for selecting anti-fraud software: have competing software vendors run a demonstration on your company's own computer database.

That was the approach taken last year by Scott Bothwell at the National Insurance Crime Bureau to evaluate anti-fraud software technologies. He salted the NICB's database with information from a sophisticated Russian fraud ring that it had stopped in 1998. He gave the database to two companies to see what they could find.

In just three days InfoGlide found the fraud ring while the other software product found nothing. The similarity search engine was able to search several dozen fields besides names, addresses and vehicle identification numbers to find the clever criminal who had changed data to avoid detection. Fraud Investigator found the Russian crime gang material in the database "but it also found things we weren't aware of in our own data," Bothwell says.

NICB is a non-profit investigative agency supported by more than 1,000 U.S. property and casualty insurance companies. Bothwell advises any company to do what NICB did – have various vendors do pilot studies using their own company data and then judge the results. "Some software packages are very expensive so you want to make sure what you buy will work," he says. ■

Card Tricks

ILLUSTRATION BY JOSH LEIPCIGER

Losses from credit card, debit card and ATM fraud exceed more than a billion dollars annually in the U.S. alone. But the problem is no longer a national one, as an expert tells us. It's now become an international crime.

JOE MAJKA (pronounced My-kah) is a Regional Director for Visa U.S.A.'s Risk Management Fraud Control Department. He has over 24 years experience in corporate security and criminal investigations, specializing in the area of financial crime, and is certified by the American Society of Industrial Security as a Certified Protection Professional. During his career, Majka has been Director of Security for Eurekabank and Corporate Security Manager for Homefed Bank, in San Diego. He holds a Bachelor's degree from California State University, Hayward and a lifetime teaching credential from the University of California at Berkeley.

ROF: *From Visa's perspective, how serious a problem is fraud?*
JM: It's very serious. Overall, fraud increased last year, from the previous year, by approximately 14 per cent. However, I should also say that for Visa, in terms of fraud to sales volume, fraud only represents 6 cents for every one hundred dollars in sales volume, or .06 per cent.

ROF: *Many of the crimes related to the fraud losses have some kind of international connection.*
JM: That's exactly right. From a banking and law enforcement perspective, if you are still thinking locally you are behind already, because the crooks are thinking globally. And, to no surprise, the Internet is bringing them to you. In the past, a merchant was used to doing business locally or maybe state wide. Most customers would walk into the business to conduct their transactions. The Internet takes that all away. Today, you can be doing business with somebody in the UK or Russia or Latin America. They don't have to walk into your store any more. And the criminals are using that to their advantage.

ROF: *Can you give an example?*
JM: A Wisconsin merchant received an order from Belarus, part of the former Soviet Union, for 50,000 pentium chips. The guy in Belarus gave a credit card number that he'd obtained from a fraud program available on the Internet called CreditMaster. The merchant called his bank and got authorization and shipped the stuff out. Now you and I might be a little suspect about sending a first order of 50,000 chips to someone in Belarus that you've never done business with before. But the merchant wasn't. After it was too late, it was discovered that the card number, which was from Canada, had been stolen.

ROF: *How did that happen?*

JM: CreditMaster, which anyone who surfs the Net can find, was developed in 1992 by a group of hackers who decided to have fun with the financial industry. It's in version 4.0 now. This program allows you to generate credit card and debit card account numbers. The way it works best is to take one good account number, which can be obtained off a receipt. They know that the first four to six numbers identify whether it's a Visa, Mastercard, American Express or Discovery number. They put the number into a program and ask it to give them 999 account numbers, half above and half below the good number. The program then generates a number, usually 13-16 digits, that meet a very simple algorithm used in the banking industry to create a credit card number. It's that simple.

ROF: *But they don't know if the numbers are legitimate.*

JM: No they don't. But if a bank issues their numbers sequentially, which many of them do, chances are they're going to come up with a lot of good numbers. Then what they do is test the number out. For example, they call AOL and if they can open up an account with that number, then it's good. Or, they transfer the number to a piece of plastic and go to a gas station where you can pay at the pump with a credit card. And, as one of my colleagues likes to say, if it passes gas then they know they can go ahead and commit fraud.

ROF: *How else are numbers stolen these days?*

JM: The most current method is something called skimming. If you remember a few years ago, crooks were stealing credit card numbers by copying them off a restaurant receipt, for example. To combat that, the industry put this little three-digit number on a card's magnetic stripe, which didn't show up on the receipt. If it wasn't on an authorization, the transaction was refused. But the crooks now have a device that we call a wedge. It can be as small as a pack of cigarettes or a pager. If they take your card, typically at a restaurant, and swipe it through the device, it stores everything on the card: your name, number and the three-digit code. They then download that onto their computer and transfer it onto a counterfeit card. You still have your card in your wallet. It hasn't been stolen or lost but the crooks can use it. Often somewhere far away.

ROF: *Where have stolen U.S. card numbers turned up?*

JM: The crooks often email the numbers outside the country. We have found numbers skimmed from a restaurant in Virginia on some suspects arrested in Taiwan. They were linked to individuals selling skimming devices in Japan, Malaysia, Korea and the U.S. Interestingly, they used the Royal Bank logo on all their plastic. Another example was a little Chinese restaurant in Wilson, Oregon. Within three to five days after skimming customers' numbers, those numbers showed up in Beijing, China. Months later we saw the same numbers in Chicago and Latin America.

ROF: *As a recent case in Canada revealed, skimming also takes place at ATM machines.*

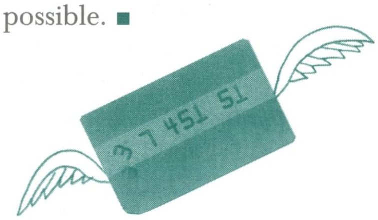
JM: That's right. Last year some Russian nationals arrested in Sweden had equipment on them that they would lay over the PIN pad of an ATM machine. When you entered your PIN number it would capture it. They also put a device on the face of the machine that would capture everything on your card.

ROF: *Are mostly amateurs or organized criminals involved in this?*

JM: Both, but increasingly we see international organized crime. And they're using the profits from this type of fraud to fund other activities, such as drugs and guns. About two years ago in southern California, a highway patrolman was shot and killed when he made a routine traffic stop. In the trunk of the car were counterfeit travellers' cheques. The person who shot and killed him was a member of an Asian organized crime group. That's how serious this business is. I met with the Secret Service recently and they were telling us everything lately involving these kinds of frauds seems to come back to Hong Kong, Vancouver and San Francisco. There's always that connection there.

ROF: *Can you stop this kind of fraud?*

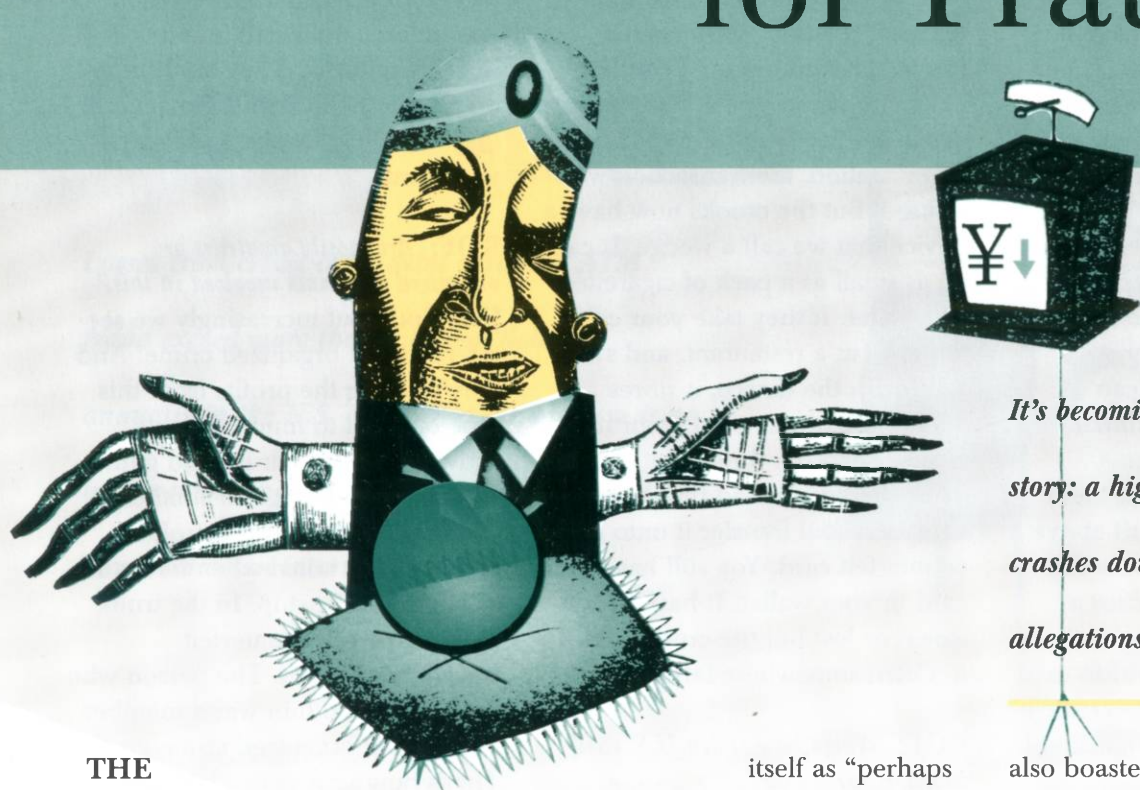
JM: We can and we're working on ways right now. But whatever we come up with, the crooks will likely find a way to crack it. What we hope to do is stay ahead of them for as long as we can, and to keep the losses down to as minimum a level as possible. ■



REPORT ON **Fraud**

A *Yen* for Fraud

by Jock Ferguson



It's becoming an all too familiar story: a high flying financial wizard crashes down to earth amid allegations of wrongdoing.

THE LATEST FALLEN hero is Martin A. Armstrong, the head of the Princeton Economic Institute (located in Princeton, N.J., but not connected to Princeton University), who was charged last fall by the U.S. Attorney of the Southern District of New York with "a massive scheme through which billions of dollars of promissory notes were fraudulently sold to Japanese corporate investors." The same day the U.S. Securities and Exchange Commission (SEC) filed a civil action and obtained an injunction to freeze his assets, stop him carrying on business and appoint a receiver to take over his companies. Armstrong is currently out on $5-million bail.

Prior to the charges, the Princeton Economic Institute billed itself as "perhaps the largest global advisory firm in the world to major multinationals, governments and institutions."

Made His Stamp at Age 13

A child prodigy, Armstrong, now 49, began his career as a 13-year-old stamp dealer. The author of several influential books on stamp collecting, he was drummed out of the philatelic community in 1972 after being accused of having sold rare stamps that he didn't own.

Undaunted, Armstrong reinvented himself over the next two decades as a financial guru, establishing an impressive-sounding legend. He claimed that his $60-million artificial intelligence forecasting system correctly predicted crashes in the U.S. stock and bond markets in 1987 and 1994 respectively. He also boasted how he had correctly forecasted the steep downturn in the Japanese economy in 1989, and more recent fluctuations in the value of the yen against the U.S. dollar. His web site showed a picture of him with former UK prime minister Margaret Thatcher in 1996.

His stellar reputation as an economic forecasting guru attracted well-heeled institutional investors, particularly from Japan. In the last half of the 1990s they gave his Tokyo office more than $3 billion to manage.

Ponzi Scheme

The breaks were applied to Armstrong's wild ride when he was charged with criminally masterminding an international Ponzi scheme that defrauded his Japanese corporate investors of close to US$1 billion.

ILLUSTRATION BY JOSH LEIPCIGER

Documents filed in criminal and civil proceedings show a vast chasm between appearance and reality, a gulf that is embarrassing for professional advisors and executives deceived in the scam, as there is little evidence of thorough due diligence by investors. The case illustrates vividly the inherent dangers of entrusting money with people who promise greater returns than those being offered by most of the market.

Investors thought Armstrong had unique economic forecasting expertise that other money managers lacked, giving them an advantage that would produce higher returns. His crystal ball skills, he claimed, had produced an average annual return of 28 per cent for six consecutive years, a performance that would double investors' money in just three years. At the time, Japanese banks were paying zero interest. Armstrong promised a minimum of four per cent annual return with an upside potential for much more.

A key to the façade were regular reporting letters sent to investors that falsely claimed they were earning large returns. In fact, for almost two years Armstrong's trading activity produced dramatic losses of at least $500 million.

The greatest losses were in the 18 months prior to his arrest. As the yen grew stronger and stronger, Armstrong became more desperate. Still convinced of his own forecasting rhetoric, he bet the U.S. dollar heavily against the yen. It was a dreadful mistake. Most investors bought into his deals in U.S. dollars and were to be paid back in yen. This significantly compounded Armstrong's problem. Deals that had a stated interest rate of four per cent were in fact owed over twenty per cent with the rise in the value of the yen against the dollar.

It's fascinating to go back and look at Armstrong's published views on the Japanese yen during those 18 months in 1998 and 1999. He appeared to have used his writings to try and stem the yen's downward flow. In July 1999, for example, Armstrong engaged in some self-serving warning that if the yen closed below 110.65 yen to the dollar, then it could "result in an economic catastrophe. Such a decline in the dollar will wipe out any sign of economic recovery and plunge Japan into yet another massive round of deflation. This would most likely impact the entire Asian region and at the same time perhaps push China over the edge." But in the end, it was Armstrong who fell.

"Someday I want to be rich. Some people get so rich they lose all respect for humanity. That's how rich I want to be."

– Rita Rudner

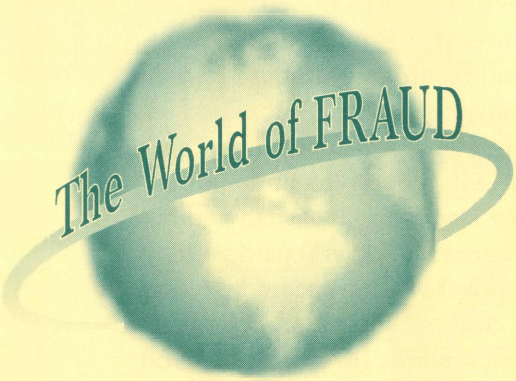
When the FBI raided Armstrong's Princeton office they found records showing obligations to repay between $700 million and $1 billion at a time when there was only $46 million left in the kitty. They also found that many early investors had been repaid with funds raised from recent investors, the classic hallmark of a criminal Ponzi scheme. Investigators found at least 113 separate investment accounts under Armstrong's umbrella and one company, Alps Electric Company, could lose as much as $185 million this year, Bloomberg News reported. It's not yet been determined how much Armstrong pocketed in management and performance fees or where that money is located.

Says He's a Scapegoat

Armstrong strongly denies the criminal allegations. His lawyer was quoted as saying that Armstrong is being made a scapegoat for "honest non-criminal trading losses."

No matter how the criminal and civil proceedings resolve, it is obvious that many investors – including upward of 80 Japanese companies – put their blind faith in Armstrong's self-proclaimed genius. Just as there are too many stories lately of financial gurus who may be anything but, there are even more examples of supposedly sophisticated investors who failed to look beneath the surface to determine whether a deal that seemed too good to be true was in fact just that. ■

Jock Ferguson is a Toronto writer.



A selection of fraud stories culled from around the globe

A Really Sick Fraud

Bobby Heaton fleeced five investors of $6,100 late last year from a scam he ran out of his hospital bed. Heaton, who used a fake name, pretended to have had a heart attack to get into St. Joseph's Hospital in Houston. Then he convinced a pastor's wife, who counseled the ill, to get her friends to invest in a scheme that promised them a 600 per cent return on their money. Heaton not only fled with their money, but left without paying his $41,000 medical bill.

Soccer Fraud Balls-Up

Twenty-two football players with Newcastle United were double-crossed by a scalper last December after they tried to sell their complimentary FA Cup Final tickets, with a face value of £36, for £450 each. When reserve goalkeeper Peter Keen, who was the plan's mastermind, returned from handing over the tickets to the scalper, he discovered the payment envelope contained only Monopoly money. According to *The Mirror*, some of the players, many of whom earn thousands of pounds a week, wanted the money to pay for vacations with their girlfriends.

Send Him to Sing Sing

Ever thought of filling out more than one of those offers from music companies that send you up to a dozen CDs for the price of one? David Russo, 33, of New Jersey sure did. Over a four-year period, Russo opened 1,630 fake accounts with BMG Music Services and Columbia House. He used the 22,260 CDs, worth about $350,000, to stock his flea-market booths. Russo, who paid about $50,000 for the CDs that he had sent to post-office boxes under false names, was charged with mail fraud.

Get Your Money Smelling Pacific Ocean Fresh

How can Nauru, an eight-square-mile coral island in the Pacific Ocean near Australia, have one of the highest per capita incomes in the world? By doing laundry for the Russian Mafia. According to *The Sunday Times of London*, the Russian mob washed about US$70 billion worth of dirty money through the island's 200 banks last year. Nauru's inhabitants were already wealthy from the island's fossilized, phosphate-rich bird droppings. They are now even better off, thanks to a different kind of deposit: proceeds from drug trafficking, prostitution and people smuggling. ■

Feedback

Report on Fraud welcomes all letters and comments. Please address comments to:

Peter Hoult, CA, Director, Information and Productivity Resources
Member Services
The Canadian Institute of Chartered Accountants
277 Wellington Street West
Toronto, Ontario
Canada M5V 3H2
Telephone: (416) 204-3330
Email: peter.hoult@cica.ca

Paul McLaughlin, Editor
Kroll Lindquist Avey
One Financial Place
One Adelaide St. East
Toronto, Ontario
Canada M5C 2V9
Telephone: (416) 956-5011
Email: pmclaugh@kroll-ogara.com

Murray B. Schwartzberg, JD, Technical Manager
American Institute of Certified Public Accountants
Harborside Financial Center, 201 Plaza Three
Jersey City, NJ 07311-3881
Telephone: (201) 938-3194
Email: mschwartzberg@aicpa.org

Unsolicited manuscripts on matters dealing with fraud are welcome and will be considered for publication.

Filing Instructions

AICPA

The CPA's Handbook of Fraud and Commercial Crime Prevention

Supplement 1

March 2001

Dear Subscriber:

Enclosed is the March 2001 Supplement, your first annual supplement, to your *CPA's Handbook of Fraud and Commercial Crime Prevention.* You will continue to receive your bi-monthly *Report on Fraud* newsletter. Your 2001 Supplement includes the following important features.

New Chapter

Financial statements, sensitive areas for practitioners, are tied so closely to a CPA's activities that any hint of fraudulent practices cannot be overlooked. Whether the motivation for fiddling with financial statements is an effort to hide a business's worth in a messy divorce or an attempt to induce a lender to extend further credit, the CPA's role is pivotal. We have added a **completely new** *Handbook* chapter, "Reducing the Risk of Financial Statement Fraud," by Charles Lundelius, Jr., CPA, ABV, BS, MBA, of Kroll Lindquist Avey, Washington, D.C. The *Handbook's* new chapter has been carefully constructed to bring together all the key issues and considerations to assist you in meeting your clients' requirements or carrying out your staff responsibilities.

The new chapter includes the following:

- **The pervasive nature of financial statement fraud,** exploring the most common financial statement frauds and who is most likely to attempt the fraud

- **The kinds of financial statement fraud,** describing earnings manipulation and management, balance sheet manipulation, and problems of closely held entities

- **The predictors of financial statement fraud,** explaining both quantitative and qualitative predictors and how to apply them

- **The special areas of financial statement fraud,** delving into matters such as loss contingencies, asset write-offs, the role of acquisition reserves, and fictitious revenues

- **The financial statement fraud checklist,** which is a ready-to-use tool that assists you in covering the bases in your fight to reduce the risk of financial statement fraud

New Diskette

Your supplement includes a new Microsoft® Word diskette containing the **Financial Statement Fraud Checklist** in addition to all the other checklists and fraud vulnerability grids from your old diskette. You can download and adapt the new **checklist** to meet specific client or organizational needs.

056550

New Sector-by-Sector Introductions

Your supplement includes expanded introductions to two of the business sectors found in Appendix A:

- The new **Financial Services** Sector introduction exposes the potential attack points for the fraudster in this multi-faceted industry, which is where the money is: **banking, insurance, securities, and mutual funds.** Because this sector cannot be divorced from money in all its iterations, fraudsters make it their prime point of attack. This new information will help you to install the fraud-reducing controls for both the financial services industry and its customers.

- The new **High-Technology** Sector introduction zeroes in on the fraudsters' targets: businesses that develop high-technology products or use high-technology to produce their products. Fraudsters can attack these businesses using new techniques—computer invasion—or old scams modified for new technologies. To help you strike a blow against the fraudsters, your new information highlights the controls you can use to combat the internal or external high-tech fraudster.

New Developments

Your supplement contains multiple **replacement pages** containing information on **new developments** in fraud awareness and highlighting the controls that should be considered in the constant fight against the fraudster.

Glossary and Bibliography

The new **Glossary** and **Bibliography** have more references for your information.

Report on Fraud

You will also continue to receive the ***Report on Fraud*** as part of your subscription to *The CPA's Handbook of Fraud and Commercial Crime Prevention.* This bi-monthly newsletter keeps you current on the newest, worldwide fraud developments.

Contact Us

If you have any questions regarding your subscription or any other AICPA product, please call the AICPA Member Satisfaction Team at (888) 777-7077, where any agent will be pleased to assist you. Or you may email your questions to memsat@aicpa.org.

As always, thank you for giving us the opportunity to provide timely and practical professional information.

Sincerely,

Linda Prentice Cohen

Linda Prentice Cohen
Publisher
Professional Publications & Technology Products

AICPA SOFTWARE LICENSE AGREEMENT

The CPA's Handbook of Fraud and Commercial Crime Prevention
Supplement 1—3/01

LICENSE AGREEMENT

The disk provided with *The CPA's Handbook of Fraud and Commercial Crime Prevention* contains electronic versions of the checklists found in the book. Subject to the conditions in this License Agreement and the Limited Warranty herein, you may duplicate the files on this disk and/or modify them as necessary **for internal use only**.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, for purposes other than internal use without the prior written permission of the AICPA.

Limited Warranty

AICPA warrants that the program will substantially conform to the published specifications and to the documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. AICPA also warrants that the magnetic media on which the program is distributed and the documentation are free from defects in materials and workmanship. AICPA will replace defective media at no charge, provided you return the item with the original packaging with the book to AICPA within 90 days of the date of delivery.

Except as specifically provided above, AICPA makes no warranty or representation, either express or implied, with respect to this program or documentation.

In no event will AICPA be liable for direct, indirect, special incidental, or consequential damages arising out of the use of or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, AICPA is not responsible for any costs including, but not limited to, those incurred as a result of lost profits or revenue, loss of use of the computer program, loss of data, the costs of recovering such programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. In no case shall AICPA's liability exceed the amount of the license fee (i.e., cost of product).

The warranty and remedies set forth above are exclusive and in lieu of all others, oral or written, express or implied. No AICPA dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty.

Some states do not allow the exclusion or limitation of implied warranties or limitation for incidental or consequential damages, so the above limitation or exclusion may not apply to you. In the U.K., this warranty does not affect the statutory rights of a consumer.

General

The material on this disk is designed to provide information in regard to the subject matter covered and does not represent an official position of the American Institute of Certified Public Accountants, and it is distributed with the understanding that the publisher, authors, and editors are not rendering legal, accounting, or other professional services on this disk. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

AICPA retains all rights not expressly granted. Nothing in this License Agreement constitutes a waiver of AICPA's rights under the copyright laws or any other Federal or State law.

Installation of the Fraud Handbook Companion Diskette

How to Install and Use the disk:
There are numerous ways to open, copy, and save files. Use the method you prefer. Refer to your computer's user manual for help with saving and opening files if needed. These directions are generic in nature and not specific to all computers or user preferences.

Installing: Open Word 97 on your screen and insert the companion disk into your computer's disk drive (a or b) and wait to click. Go to the file button and select *open* (with disk drive a or b selected). A list of files will appear. *All files* or *Word Documents* should be selected in dialog box. Select the file you want to open. You can now work on the file you have selected. The Sector-by-Sector checklists can be found in the Sector-by-Sector folder.

Note on Fonts: The exhibits on disk were produced in Word for Windows 97 using True Type fonts. If you do not have this font library available, the exhibits may not convert correctly. You will have to substitute a different font and may have to replace/correct formatting that does not convert correctly.

Saving: If you plan to continually use and update the template file with client or other information, you must use the *Save As* feature when saving the file with new information for the first time. Go to the File button and select *Save As*. Save the file selected under a new name that you will remember for later use. Direct the saved file to your hard drive or other location as appropriate for your needs.

Note to Users: As a general rule, remember to save your data frequently. Note that *The CPA's Handbook of Fraud and Commercial Crime Prevention* checklists were produced to be used as template documents only. In order to maintain the template, you must save your work under the *Save As* window the first time you use a document and give your work a different name. This will allow you to always have the template available and to continue to customize the forms as needed.

Warning: If you use the *Save* function the first time you save your work, you will overwrite the template. This means that you will have to clean up your saved file to return it to template status or reload the file from the disk.

The CPA's Handbook of Fraud and Commercial Crime Prevention

Updating Letter—Supplement 1—3/01

Page Description	Discard These Handbook Pages (Chapter/Page)	Insert These Supplement Pages (Chapter/Page)
Title Page	Title Page	Title Page
Table of Contents	iii	iii
Preface	v to viii	v to viii
Acknowledgments	ix	ix
About the Authors	xi to xiii	xi to xiii
Chapter One: "Managing the Risk of Fraud"	7 to 8	7 to 8
	11 to 12	11 to 12
	17 to 20	17 to 20.1
Chapter Two: "Promoting an Ethical Environment"	5 to 6	5 to 6
Chapter Four: "Computer Security"	23 to 27	23 to 27
Chapter 5: "Internal Fraud"	3 to 4	3 to 4
	15 to 18	15 to 18
	21 to 22	21 to 22
	25 to 32	25 to 32
Chapter Six: "External Fraud"	TOC page	TOC page
	3 to 4	3 to 4.1
	11 to 14	11 to 14.1
	29 to 32	29 to 32
Chapter Seven: "Commercial Crime"	17 to 18	17 to 18
	21 to 24	21 to 24
	29 to 30	29 to 30

Page Description	**Discard These Handbook Pages (Chapter/Page)**	**Insert These Supplement Pages (Chapter/Page)**
Chapter Nine: "Dealing With Fraud"	9 to 10	9 to 10.1
Chapter 10: "Reducing the Risk of Financial Statement Fraud"	———	Insert new tab card and chapter 10 text pages 1 to 70 immediately following chapter 9.
Appendix A: "Fraud Sector-By-Sector"		
Section 2: "Financial Services"	9 to 10	9 to 10.13
Section 4: "High Technology"	21 to 22	21 to 22.14
"Glossary"	1 to 37	1 to 35
"Bibliography"	1 to 5	1 to 5
NOTE: A 2001 *CPA's Handbook of Fraud and Commercial Crime Prevention Checklists* diskette is included with Supplement 1. It replaces the previous version in its entirety.		

This completes the filing of Fraud Supplement One.

Upon completion, insert this Update Letter behind the "Filing Instructions" tab card included with your supplement. It should be inserted immediately after the "Report on Fraud" tab card.