1-1-1984

Report on the study of EDP-related fraud in the banking and insurance industries

American Institute of Certified Public Accountants. EDP Fraud Review Task Force

Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries

EDP Fraud Review Task Force

AICPA

Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries

EDP Fraud Review Task Force

American Institute of
Certified Public Accountants

Notice to Readers

This report is issued by the American Institute of Certified Public Accountants for the information of its members and other interested parties. However, this report does not represent an official position of any of the Institute's senior technical committees.

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

Preface

Crimes and catastrophes make eye-catching headlines. Stories that include large sums of money, intrigue, technology, and clever schemes are good copy. Frauds involving electronic data processing (EDP) often have all these features. Cases such as the $200 million insurance fraud at Equity Funding, the $21 million theft at Wells Fargo Bank, the $24 million misstatement of revenue at JWT Group, Inc., and the $10 million wire transfer theft from Security Pacific National Bank all received national attention.

These cases share some common characteristics. The perpetrators were individuals familiar with the companies' systems; their objectives were to either carry out or conceal financial misdeeds; and they took advantage of the existing technology.

There has also been press coverage of break-ins to computer systems for reasons other than to commit fraud or theft. Although these acts point out potential security problems, they are not related to the business fraud cases reviewed in this study.

The purpose of this report is to place the problem of EDP-related fraud in perspective. Because of the inadequate data available on many reported cases, it is difficult to determine what went wrong or how the crime could have been prevented. By describing the specifics of how several cases were perpetrated, the Task Force hopes to provide information that will help EDP users prevent becoming victims of similar frauds.

Acknowledgments

The Task Force is indebted to the Bank Administration Institute, the American Insurance Association, the American Council of Life Insurance, and the Life Office Management Association for their support of this project. The Task Force particularly thanks those banks and insurance companies that cooperated in the surveys and were willing to share their experiences.

Membership

EDP Fraud Review Task Force

CARL A. PABST, *Chairman*
BRANDT R. ALLEN
BILL D. COLVIN
FREDERICK L. NEUMANN
JAMES R. WATTS
ROGER J. WHEELER
JAMES L. BROWN
WILLIAM J. DUANE
STEPHEN W. C. HOLBROOK
MARK F. POLANIS
JOAN TARWATER

Sub-Task Force for the Survey of the Insurance Industry

JAMES R. WATTS, *Chairman*
CHARLES A. ANDERSON
WILLIAM C. FREDA
JOHN C. GAZLAY
OTTO K. KALOK

AICPA Staff

DAN M. GUY, *Vice President, Auditing*
NANCY A. FOX, *Practice Fellow, Auditing Standards*
MICHAEL F. GRIES, *Practice Fellow, Auditing Standards*

Contents

Introduction

Background

Growth in the use of large integrated data bases, microcomputers, portable "intelligent" terminals with access through telecommunications, and other evolving technologies, can provide greater susceptibility to fraud. The increasing complexity of computer systems and their related operations compound the difficulties of preventing and detecting fraud.

The concentration of processing and recording activities in computer systems makes the accounting records of some organizations more accessible and the manipulation of those records and the concealment of theft somewhat easier. The decreasing use of hard copy books, records, and other documents and decreasing human involvement also facilitates concealment. The ability to alter data in computer systems, often without any observable evidence of manipulation, has made it easier to perpetrate and cover up fraud.

Because of the significant potential for EDP-related fraud, the American Institute of Certified Public Accountants (AICPA), in 1978, appointed the EDP Fraud Review Task Force to look into the nature and pervasiveness of such fraud. The Task Force evaluated several sources of information and reviewed several cases in depth. The Task Force was unable to obtain significant information from existing or potentially available sources. This was primarily due to a lack of consistent, comprehensive, reliable data and a reluctance or inability of the sources to disclose significant facts.

To obtain information for analysis, a study consisting of two industry surveys was undertaken, focusing attention on the variety of fraud scenarios to provide a basis for evaluating the range of conditions through which EDP-related frauds may occur. The focus of this study was on the who, what, where, when, why, and how of specific EDP-related fraud cases rather than on projections of the number of cases or the dollar size of those cases. For this reason, readers are cautioned not to generalize or

draw conclusions on the incidence or dollar magnitude of EDP-related frauds based on the results of this study.

The extent of EDP-related fraud may not be quantifiable for a variety of reasons. There is a lack of reliable data. Available data is frequently based on news coverage. Legal constraints prevent comprehensive analysis of some cases until court proceedings are complete. Not all reports of fraud accurately distinguish frauds related to EDP, and, in fact, there is no general agreement on the definition of EDP-related fraud. There is also a general reluctance of many companies to disclose information about fraud.

Furthermore, determining the size of the problem may be affected by the following factors. First, several cases of EDP-related fraud continue for long periods of time — some for many years — before they are detected. Some may never be detected; thus, undetected frauds are likely to exist, but their number and magnitude are unknown. Second, many EDP-related frauds are discovered accidentally. Thus, the dollar amount of reported frauds merely states the minimum amount; the potential total loss is considerably higher. Third, the amount of the loss may be stated either before or after restitution, or it may be the amount manipulated or only the actual amount extracted.

Auditors' Concern with EDP-Related Fraud

Traditionally, independent auditors have been engaged to lend credibility to the financial statements they examine. Users of those audited financial statements expect that they can reasonably rely on such statements for making economic decisions. Therefore, auditors are concerned about matters that can *materially* affect the reliability of the financial statements under examination.

Fraud or irregularities could have a material effect on the financial statements. The AICPA's position on auditors' responsibilities for the detection of fraud is stated in Statement on Auditing Standards No. 16:[1]

> Under generally accepted auditing standards the independent auditor has the responsibility, within the inherent limitations of the auditing process . . ., to plan his examination . . . to search for errors or irregularities that would have a *material* effect on the financial statements, and to exercise due skill and care in the conduct of that examination . . . . An indepen-

[1]AICPA, Statement on Auditing Standards No. 16, *The Independent Auditor's Responsibility for the Detection of Errors or Irregularities* (New York: AICPA, 1977), paragraph 5.

dent auditor's standard report implicitly indicates his belief that the financial statements taken as a whole are not materially misstated as a result of errors or irregularities.[2] (emphasis added)

Because information used in the preparation of financial statements is often processed by computers, auditors are concerned with errors and irregularities that might occur during computer processing that could have a material effect on the financial statements.

Definition of EDP-Related Fraud

The Task Force's definition of EDP-related fraud used for this study was "any intentional act, or series of acts, that is designed to deceive or mislead others and that has an impact or potential impact on an organization's financial statements. EDP must be involved in the perpetration or cover-up of the act or series of acts." This definition has three essential characteristics.

1. *The existence of fraud.* A good definition of fraud is that given in the report of the Commission on Auditors' Responsibilities:[3]

   Viewed broadly, any intentional act designed to deceive or mislead others is fraud. Fraud in the business environment with which the auditor is concerned has a more specialized meaning. Fraud may occur at the employee or management level. Frauds by nonmanagement employees are generally designed to convert cash or other assets to an employee's own benefit. . . . Fraud at the management level includes intentional misrepresentations that may lead to improper selection of accounting principles or inclusion of false amounts in, or the omission of amounts from, financial statements. It is usually accompanied by acts of concealment, such as omission of entries, manipulation of documents (including forgery), or collusion among individuals inside or outside the company.

2. *An impact on the financial statements.* Fraud can affect financial statements in a variety of ways:

   - Theft, impairment, or misrepresentation of assets
   - Misrepresentation, omission, or concealment of liabilities or equities
   - Manipulation or misrepresentation of revenue or expenses

[2]Irregularities are defined by SAS No. 16 as intentional distortions of financial statements or misappropriations of assets.

[3]*Commission on Auditors' Responsibilities: Report, Conclusions, and Recommendations* (New York: AICPA, 1978), page 32.

3. *Involvement of EDP*. The third and essential characteristic of the definition of EDP-related fraud used for the study is that EDP must be directly involved in the perpetration or cover-up of the scheme. EDP may be directly involved by any improper manipulation of:

   Input or transaction data — Manipulations may occur when unauthorized data are prepared for input to a computer system or when authorized input is improperly altered, duplicated, destroyed, or withheld.

   Output or results — Manipulations may happen when reports, files, or other output are mislabeled, misrepresented, altered, or misdelivered to effect a fraud or cover-up.

   Application programs — Manipulations may be accomplished by the development of unauthorized programs, or segments of programs, or by the subsequent alteration of once-acceptable programs or documentation.

   Data files — Manipulations may happen when files are directly changed without transactions, such as through the use of file utilities or on-line terminal access.

   Computer operations — Manipulations may result from the deliberate misuse of the computer system operations such as the use of the wrong programs, data files or transactions, or the interruption of normal program processing.

   Communications — Manipulations may happen by intervention in the process of data being sent between terminals and the computer or between two or more computers.

   Computer hardware, systems software or firmware — Manipulations may happen by improper use, alteration, or intervention in the functioning of these resources.

Other definitions of EDP-related fraud have included theft of software, hardware, or data; theft of computer time; and errors (made without the intent to deceive). The definition used for this study specifically excluded those occurrences, as well as other computer crimes or abuses, such as the destruction of computer software or hardware or illegal access to telecommunications or computer systems without the intent to commit fraud.

The Study

To study EDP-related fraud, surveys were conducted in the banking and insurance industries in cooperation with the Bank Administration Institute, the American Insurance Association, the American Council of Life Insurance, and the Life Office Management Association. These industries were selected because both are highly automated, both deal in liquid assets, and the operations of entities within each industry are fairly similar.

Similar questionnaires were sent to banks and insurance companies. No respondent identification techniques were used, although respondents were invited to identify themselves to permit follow-up inquiry. In some cases, the Task Force contacted banks and insurance companies that had identified themselves, to obtain additional information to complete the analysis.

It should be noted that survey participation was voluntary. The Task Force was aware of some significant cases that were not reported through the surveys and could, therefore, not be included in the study.

Of the 9,405 banks surveyed, 5,127 responded, yielding a response rate of 55 percent. Of those responding, 105 reported they had experienced at least one case of what was believed to be EDP-related fraud and submitted information on one of their cases. After reviewing the details of all reported cases, it was determined that 85 conformed to the study definition.

The insurance company questionnaire was sent to 1,232 companies, 429 were casualty-property insurance companies, and 803 were life and health insurance companies. A total of 854 responded, for a response rate of 69 percent. The respondents identified 40 cases they believed to be EDP-related fraud. Of the cases submitted, 34 conformed to the study definition.

The data and analyses provided in the following sections, although presented in some cases in a numerical format, are not intended to present conclusions about the incidence or magnitude but rather on the general nature and means of committing some EDP-related frauds.

Summary of Findings

The 119 cases identified in the surveys of EDP-related fraud in the banking and insurance industries provide useful information for devising strategies for preventing and detecting EDP-related fraud. The results of the surveys are categorized to answer the following questions:

- What was the environment in which the frauds were committed?
- What was the general nature of the frauds, and how were they committed?
- Who committed the frauds, why, and what corrective action was taken?
- How were the frauds detected?

What Was the Environment in Which the Frauds Were Committed?

In almost all cases, the fraud occurred during normal transaction processing cycles. The type of computer system was not significant. Also, fraud occurred in both batch and on-line systems. It should be noted, however, that at the time of the surveys the insurance industry used on-line systems more than the banking industry did. This accounts for some industry differences in the analyses. Many types of application systems were subject to manipulation.

What Was the General Nature of the Frauds, and How Were They Committed?

Perpetrators employed a variety of schemes, methods, and techniques. Relatively few perpetrators used sophisticated techniques; many took advantage of weaknesses in the system of internal accounting control. Inadequate segregation of duties was a common weakness in the reported frauds.

Most frauds were perpetrated in the input area; perpetrators generally introduced or created unauthorized input or manipulated otherwise proper input. File maintenance was a fairly common method used by perpetrators; in all but one of these cases, the file maintenance manipulation involved nonfinancial data (for example, extending due dates on loans, changing names and addresses).

A specific area worthy of mention is the importance of control over access codes and passwords and, specifically in banking, the availability of personal identification numbers and the plastic cards needed to access automated teller machines.

In some cases, there appears to have been no significant attempt at concealment. It appears that the perpetrator may have relied on a large volume of transactions to cause the fraudulent transaction to be "lost." In other cases, perpetrators attempted to conceal their frauds by altering names and addresses to divert normal customer correspondence. Several cases involved over 100 transactions, but in one case, several million dollars was taken in a single transaction.

Losses from the reported cases ranged up to several million dollars, although the majority involved amounts of $25,000 or less. The amount of the loss is before any restitution.

Who Committed the Frauds, Why, and What Corrective Action Was Taken?

The cases showed the range of perpetrators covered almost every aspect of corporate operations, with the preponderance outside the EDP area. Most perpetrators in the banking industry were either data entry clerks or loan officers. In the insurance industry, most were claim processors or policy service clerks. Where perpetrators were supervisors or management personnel, their schemes generally lasted longer and involved larger dollar amounts.

In several cases, accomplices were used to receive or negotiate funds; but, in virtually all of these cases, they were not necessary to perpetrate the fraud.

The primary objective of most perpetrators was to take money from the bank or insurance company; however, some perpetrators manipulated data to show a better record of performance (for example, one bank loan officer extended due dates on loans to show a good record of loan collections).

In virtually all cases, perpetrators were employees and were later dismissed from employment. In the majority of the cases, legal action

was taken or was pending. In many cases, restitution was made or was in process.

How Were the Frauds Detected?

According to the respondents, the cases were detected by the following means:

1. Methods of detection:
   - In approximately one-third of the cases, the systems of internal accounting control or routine internal or external audits uncovered the fraud.
   - Approximately another one-third of the cases were detected through nonroutine events (such as, accident, unusual activity of perpetrator, or tip-off).
2. Sources of detection:
   - In the majority of the cases, people uncovering the frauds were within the company (that is, other employees, middle management, and internal auditors).
   - In about one-fourth of the cases, customer complaints were mostly the source within the first three months. Virtually all these cases occurred in the banking industry; in the insurance industry, policyholders usually were not aware that fraudulent transactions had been processed against their policies.

Analysis of Reported Cases

Selected characteristics of each EDP-related fraud and perpetrator were identified and summarized to present a composite profile of the 119 cases reported by the survey respondents (85 bank cases and 34 insurance cases). This section contains tables and explanations of these analyses.

Application Systems Affected

The *application system* is the primary area of operations affected by the fraud. Listed below, by industry, are the applications reported affected by the 119 cases, from most to least frequently affected.

Table 1 — Application System

Banking	*Insurance*
• Demand Deposits	• Accident and Health Claims
• Proof and Transit	• Property and Casualty Premiums
• Installment Loans	• Life Insurance Premiums/Commissions
• Credit Card Loans	• Policy Loans
• Savings Accounts	• Property and Casualty Claims
• Commercial Loans	• Life Insurance Dividends, Surrenders (Cancellations), and Other Transactions
• Automated Teller Machines	
• Check Credit	
• Cash Control	
• Mortgage Loans	
• Wire Transfer	

Banking Applications

Demand deposits are checking accounts.

Proof and transit is the verification and balancing of daily bank trans-

actions, accounting distribution of those transactions, and collection of checks and drafts payable at or through other banks.

Installment loans are single disbursement, often consumer, loans that are repaid through regular payments.

Credit card loans are revolving credit lines available to bank credit card holders.

Savings accounts refers to relatively low-rate interest-bearing deposits.

Commercial loans are typically single payment loans.

Automated teller machines (ATM) allow customers to deposit, withdraw, or transfer funds, remotely, without the involvement of a bank employee. For purposes of analysis, ATM has been categorized as a special application, distinct from the cash application.

Check credit refers to revolving credit activated by writing checks and overdrafts.

Cash control is the cash balancing function performed by tellers.

Mortgage loans are generally collateralized long-term loans.

Wire transfers are the instantaneous, electronic movements of, frequently, large amounts from accounts at the bank to other banks.

Insurance Applications

Accident and health claims cover recording, approving, and paying claims for medical expenses under group or individual accident or health insurance policies.

Property and casualty premiums includes processing of premium billings, endorsements, refunds, and cancellations.

Life insurance premiums/commissions covers processing of billings and adjustments, as well as commissions due to agents.

Policy loans refers to loans made against the cash surrender value of life insurance policies.

Property and casualty claims includes recording, approving, and paying claims for damages to property, liability for damages to the property of others, or injuries to others.

Life insurance dividends, surrenders (cancellations), and other transactions have been grouped together for purposes of this analysis.

Schemes

Scheme is the fraudulent activity used by the perpetrator to effect the fraud. The accompanying table lists the schemes reported by industry, from most to least frequent.

Table 2 — Scheme

Banking	*Insurance*
• Divert customer funds into perpetrator's own account	• Create fictitious claims
• Make unauthorized extensions of credit limits, loan due dates	• Trigger unauthorized refund or reduction of premiums
• Create fictitious loans	• Create unauthorized policy loans
• Defer recording of perpetrator's own checks and charges	• Trigger unauthorized dividend withdrawals
• Forge customer input documents (checks and withdrawals)	• Forge checks
• Make ATM extractions	• Create unauthorized mortgage loans
• Make adjustments to customer deposits	• Reinstate lapsed policies
• Divert loan payments into perpetrator's own account	• Create fictitious pension payments
• Divert customer income to perpetrator's own account	
• Wire transfer	

Banking Schemes

In the cases of fraud in the banking industry, misposting or misdirecting customer deposits, often to the perpetrator's own account, was most frequent. Other frequently used schemes included crediting loans to borrowers who never received the funds, or who, in fact, may never have existed. In several cases, perpetrators made unauthorized extensions of credit limits and loan due dates. They changed the due dates on their own loans, or they changed the due date on loans for which they were responsible to make their job performance look better.

Insurance Schemes

The most frequently used scheme in the insurance industry was generating claim payments to the perpetrator or to accomplices. Another prominent scheme was generating refunds or reductions of policy premiums, for example, by authorizing refund checks after changing policyholder names and addresses, or by cancelling policies to automatically generate policy refund checks (the checks were forged and the policies were later reinstated).

Methods

Method identifies what the perpetrator did to the automated system to initiate and carry out the fraud. Several perpetrators employed multiple methods. In these cases, the analysis identified the one method that was most instrumental in carrying out the fraud. Table 3 lists the methods used, which were similar in the banking and insurance industries.

Table 3 — Method

Method	*Banking*	*Insurance*
Transactions manipulation to:		
Create original items	16	18
Divert or capture items	21	2
Force or divert rejects	14	–
Subtotals	51	20
File maintenance changes:		
Nonfinancial fields	23	13
Financial fields	1	–
Subtotals	24	13
Direct file changes	6	1
Other	4	–
Totals	85	34

Creation of original items includes initiating transfers from customer accounts to the perpetrator's account, making adjustments to their own accounts, creating loans, submitting fraudulent claims, requesting policy loans, initiating policy dividends or refunds.

Diverting or capturing items includes incorrectly encoding or altering the encoding of items to be posted to customer deposits, assets, or fee income. Also, items such as premium receipts or the perpetrator's own checks were removed from normal processing.

To force or divert rejects, perpetrators altered magnetic ink character recognition encoding. For example, a bookkeeper changed the check digit on deposits thus interfering with their timely processing and permitting a deposit lapping scheme. Other perpetrators also incorrectly encoded previously rejected items to misdirect deposits or to capture items to prevent further processing.

File maintenance changes involved making unauthorized changes to computer-based master files. This included increasing credit limits,

changing dates, opening credit or loan accounts, reactivating closed accounts, changing names and addresses, and reinstating lapsed policies.

Direct file changes involved changing master files without any associated transaction processing or file maintenance, for example, by the misuse of file utility routines.

Procedures

Procedure describes how the perpetrator manipulated the automated system to allow the methods to work. Table 4 lists the procedures the perpetrators followed.

Table 4 — Procedure

Procedure	*Banking*	*Insurance*
Prepared forms or documents improperly	34	18
Unauthorized on-line transactions, input, or access	11	15
Prepared EDP-media improperly	24	–
Altered forms or documents authorized by someone else	7	–
Manipulated EDP-media	5	1
Unauthorized program alterations	3	–
Manipulated EDP output	1	–
Totals	85	34

In both industries, the perpetrators, generally, either introduced unauthorized transactions or altered or manipulated authorized transactions.

In nearly half the cases, input forms were prepared improperly, for example, file maintenance forms or claim data forms. In a number of other cases, on-line terminals were used to input unauthorized transactions, file maintenance entries, or to gain information necessary to effect the fraud (for example, through inquiry routines). The cases of improper preparation of EDP-media involved proof operators, key-punch operators, or machine operators, intentionally misposting or miskeying transactions or misusing suspense accounts, inter-branch transactions, or adjustments. The absence of cases in this third category in the insurance industry is a reflection of the significance of on-line processing.

Perpetrators

Perpetrator refers to the position of the person mainly responsible for the fraud. Table 5 lists the reported perpetrator, by industry, in order of frequency.

Table 5 — Perpetrator

Banking	*Insurance*
• Clerks (data entry, proof machine operators, other) • Managers (loan officers) • Data processors (operators, systems and application programmers) • Tellers • Item processors	• Clerks (claim processors, policy service, other) • Supervisors (claims, policy service, other) • Insurance agents • Systems programmers

Clerical personnel were the most frequent perpetrators reported in both industries. They often had many opportunities to perpetrate a fraud by altering, rejecting, or otherwise incorrectly processing items, as well as by introducing unauthorized items. In the banking industry, they generally included data entry clerks and proof machine operators; in the insurance industry, claim processors and policy service clerks.

In the banking industry, perpetrators reported at the clerical level were more likely to be involved in frauds in the checking, proof and transit, and savings areas. In the insurance industry, clerical personnel usually focused on claims.

The next most prominent category of perpetrator reported was mid-level management or supervisory personnel. In banking, the management personnel were generally loan officers who initiated fictitious loans or extended loan due dates. In the insurance industry, management personnel were generally clerical supervisors using any of the applications including premiums, claims, and loans.

Computer personnel (systems and applications programmers and operators) were also moderately prominent in banking, but to a lesser extent in insurance. Computer personnel tended to focus on diversion of funds in banking. However in the insurance study, a systems programmer changed certain parameters concerning his own policy.

The most common objective of the perpetrators in both industries was theft of assets. To a lesser extent, some perpetrators sought to manipulate information used by management or even the financial statements,

in order to present better performance records. Occasionally a fraud was perpetrated primarily for self-satisfaction.

Fraud Size

The emphasis of these studies focused on the circumstances of the fraud rather than the dollar magnitude of individual cases. Nevertheless, the accompanying table shows an interesting relationship between the size of the fraud and the perpetrator's position. (The dollar size is the gross amount manipulated rather than only the amount actually extracted and is before any restitution.)

Table 6 — Number of Cases by Dollar Range (thousands)

Perpetrator	*Under $25*	*$26-$100*	*More than $100*	*Total*
Banking cases				
Clerical	37	–	1	38
Managers	7	4	6	17
Data processors	9	2	2	13
Tellers	5	2	1	8
Others	5	2	2	9
	63	10	12	85
Insurance cases				
Clerical	17	3	1	21
Supervisors	2	2	5	9
Others	1	2	1	4
	20	7	7	34

Management and supervisory level personnel tended to be responsible for the larger frauds, and clerical level personnel tended to be responsible for the smaller frauds. In one case, a pension supervisor was able to extract $400,000 because he had complete control over payment transactions and related correspondence with contract holders and claimants.

Duration

Duration of the fraud refers to the length of time the fraudulent activity was occurring.

Table 7 — Relationship of Duration to Perpetrator

Perpetrator	Number of Cases Lasting: Less Than 1 Month	1 to 12 Months	More than 12 Months	Total
Banking cases				
Clerical	8	36	7	51
Supervisors/managers	1	6	12	19
EDP personnel	5	7	–	12
Others	1	1	1	3
	15	50	20	85
Insurance cases				
Clerical	4	13	4	21
Supervisors/managers	–	3	6	9
EDP personnel	–	1	–	1
Others	–	2	1	3
	4	19	11	34

Frauds perpetrated by supervisory or management personnel tended to last longer than those perpetrated by clerical personnel. In one case, a claim supervisor was able to extract money over five years because he had access to subordinates' passwords, could submit false claims for clerks to process, and could access terminals to change master file data.

Concealment

In several cases no significant attempt to conceal the fraud was apparent, such as a one-shot extraction of funds with no effort to cover up. Perpetrators appear to have been relying on the possibility that fraudulent transactions would be "overlooked" or "lost" in the larger volume of transactions normally processed or would simply be written off as unreconciled items.

When attempts at concealment had been made, the effort usually involved using file maintenance transactions or destroying or "mislaying" source documents or output documents. Frequently, addresses used for mailing customer bank statements or policyholder change notices were changed so that fraudulent transactions would not come to a customer's attention. In one case, a policy service clerk used a terminal and an error correction routine to reverse the effect of file maintenance changes submitted earlier to perpetrate the fraud. In another

case, computer-generated policyholder cancellation notices were destroyed. In still others, error or reject listings were destroyed or "mislaid."

Detection

According to the respondents, the methods and sources of detection of the fraud were as follows.

Method of Detection

Method of detection identifies the event or factor that triggered the detection of the fraud.

Table 8 — Method of Detection

Method	*Banking*	*Insurance*
Control and audit		
Internal controls	12	10
Routine audit	17	4
Customer complaint/inquiry	24	4
Unusual or non-routine events		
Accident, tip-off, unusual activity of perpetrator	11	15
Non-routine study	8	1
Change in operations, EDP, or financial statements	7	–
Unidentified	6	–
Totals	85	34

Complaints from customers were much more significant to the detection of the fraud in banking (particularly in the checking and deposit areas) due to frequent correspondence with customers. For frauds of short duration (less than four months), customer complaint/inquiry was the most significant factor in detecting the frauds. In one case, after a clerk withdrew funds from a customer's account, the clerk intercepted the customer's statements. The customer complained after one statement slipped through.

Frauds perpetrated with file maintenance changes were usually detected through internal accounting controls and audit. Frauds perpe-

trated by manipulating transactions were detected almost equally by control and audit, customer complaint/inquiry, and accident.

Source of Detection

Source of detection identifies who first discovered the fraud (or caused the fraud to be discovered).

Table 9 — Source of Detection

Source	*Banking*	*Insurance*
Other employees	23	16
Middle management	20	7
Internal auditors	20	5
Customers	16	–
External auditors/examiners	4	–
Other/unidentified	2	6
Totals	85	34

Other employees, including substitute clerks, accounting clerks, and mail clerks, among others, made up the single most significant group in detecting fraud.

The following appendix contains details of selected cases. These cases were selected to illustrate the wide range of fraud scenarios described in the surveys.

APPENDIX

Sampling of Cases From the Study

(all amounts are approximate)

Banking Cases

1. A data entry clerk manipulated the automated central information file that permitted debit cards to access unrelated customer accounts through automatic teller machines. Over 100 transactions totaling $25,000 were made within a period of less than two months. Numerous customer complaints were received about unauthorized ATM withdrawals against their accounts. These complaints triggered an investigation that discovered the fraud.

2. A computer operator using a card-driven system prepared a false set of ledger cards that increased his checking account balance and decreased a large business checking account balance, which had reached $90,000. Each month at statement preparation time, accurate statements were prepared for the customer using the correct ledger cards. After several years, the fraud was detected by an employee researching another account.

3. A data entry clerk responsible for reviewing all maintenance changes on installment loans changed the due date on his own loan. He was thereby able to extend the loan five to ten times and not make any payments. The total amount of the loan was $3,500. When the employee was transferred, he could no longer make the extensions. The loan became past due, and the fraud was discovered.

4. Unauthorized extensions of payment due dates were made over a three-year period to loans of approximately $1 million. The perpetrator, a member of senior management, thereby hid delinquencies and showed a better lending and collection record. The extensions were made by master file changes prepared by the individual, who would then remove the change forms when the work was returned from the service bureau. Regulatory examiners made an investigation when they noted there were loans shown as current without payments made or extension fees charged.

5. A data entry clerk obtained a customer's credit card and personal identification number from returned mail. He then raised the credit limit on the

terminal and obtained cash from an automatic teller machine. Over a five month period $3,000 was obtained. The customer was not aware of this, as the clerk intercepted the statements. When one statement did get to the customer, the customer's complaint triggered the detection.

6. An applications programmer analyst increased his bank account and reduced a customer's account by a file manipulation, the specific mechanism of which was not disclosed. The fraud was discovered when the customer complained. The period of concealment was less than a month and the total amount was under $1,000.

7. A proof clerk correcting rejected items keyed in a false credit to his own checking account, using a CRT terminal. The total amount involved was under $300, and the period of concealment was less than one month. One of the false credits he entered was not offset by a debit. This caused an out-of-balance situation that was traced to his account. Subsequent investigation disclosed the nature and scope of the fraud.

8. A computer operator increased the balance on his own checking account ledger card and decreased the balances for two other accounts. At statement time, he would reverse all the changes so the statements sent out would be correct.

The total amount involved in this fraud was less than $1,000 and it was concealed for two months. The fraud was detected by the EDP manager when he came into work early one day and supervised the preparation of statements before the operator had a chance to replace the improper cards. A system check that recalculated the statement balance then flagged the accounts as out-of-balance.

9. An officer who supervised operations at a branch withheld savings deposits from customer savings accounts and took cash or credited his own account as an offset. The perpetrator occasionally filled in as a teller and would sell money orders and never record them as outstanding. When a complaint was made by a customer that a deposit had not been entered, the perpetrator entered a correction charging another account with the offset. Sometimes he took cash and offset the shortage by creating an inter-branch clearing. When no response to such entries were made after five to six days by other branches, the amounts were transferred to the branch's suspense account. The perpetrator also controlled that account. For the month-end balancing they were charged to another suspense account and then transferred back after the balancing.

Concealment lasted thirteen months, and the total amount was $800,000. The EDP system was used in processing the entries and in transferring the entries from account to account thereby causing them to lose their identity. The fraud was discovered when the perpetrator was transferred to another branch. Subsequently, a customer complained about a charge to his savings account that had not been authorized. The fraudulent item was traced by another employee who found that an embezzlement had occurred.

10. The cashier of this bank was able to extend loan due dates to avoid disclosure of delinquent accounts and to conceal poor lending practices. The

total amount of the loans involved was $500,000. The fraud took place for a year. It was discovered by a loan secretary who inquired about the recurring maintenance changes extending loan due dates. Apparently, no funds were actually taken.

11. A teller misappropriated cash payments made on loans and then extended the due dates so the loans would not show up as past due. The extensions were made by preparing file maintenance change sheets. After the maintenance instructions were acted on, the individual destroyed the sheets. The total amount involved was $3,000 and the fraud was concealed for six months. The fraud was discovered by the auditors when they confirmed loan balances with borrowers.

12. A credit card clerk established fictitious card accounts and credit limits. The accounts were created, addresses changed, credit lines increased, and closed accounts reactivated by terminal entry. The cards were used for cash advances and for purchases. A total of $20,000 was involved; the period of concealment was two months. Collectors became involved in investigating some of these accounts for which statements were returned by the post office or that had exceeded their credit line. Research on undelivered statements revealed that the accounts lacked authorization and supporting documentation. Further investigation identified the perpetrator and the nature of the fraud.

13. A note clerk working with a customer as an accomplice changed that customer's overdraft limit via on-line terminal input. The maintenance code to do this was supposedly known only by senior management. Approvals were forged on the input document. This customer was then allowed to draw up to $6,000 against the improperly authorized credit line. The fraud was concealed for three months. Payments were made by other unauthorized advances that were not properly shown on the reconciliation of the account. The accomplice made the mistake of calling the bank several times inquiring about the amount of his credit limit. This aroused the suspicion of the note supervisor, who couldn't understand why a customer would call several times concerning his credit limit. Upon investigation, it was found that the $6,000 credit limit had not been properly approved. Further investigation identified the scheme and the perpetrators.

14. The money transfer department received instructions from an imposter to transfer $5 million. The imposter identified himself as an employee of a branch and stated that he had received instructions from a customer to transfer the money to another institution for further transfer to that institution's customer. The test code reported by the imposter for that date and branch were correct, thereby not causing suspicion. The following morning the customer, upon receiving notification of the transaction, disputed the item and denied authorizing it. Upon inquiry, the branch reported that they never issued such instructions.

15. In this case, a branch manager and a computer operator colluded to extract cash from an automatic teller machine. The branch manager stole the money from the machine while the computer operator destroyed logs and

records of transactions transmitted from the machine to the computer center. The money was taken in small amounts over a period of four months. Between 10 and 100 shortages were involved totaling $3,500. An investigation of the cash shortages revealed the scheme between the branch manager and the computer operator. The fraud was concealed for four months.

16. An applications programmer using a terminal altered the computer programs governing the bank's cash management service. This program automatically triggered reports of excess funds, which were then to be transferred by wire to another bank. Very likely, they were credited to his own account rather than wired elsewhere. The fraud was discovered within a month because the fraudulent transfers caused overdrafts to customers' accounts. When the overdraft unit investigated disputed transactions, it discovered differences between the customer's instructions and the automatic charges. After the internal audit department investigated, the scheme and the perpetrator were identified. Between five and ten transactions were involved. The total amount of the fraud was $600,000, but no money was extracted from the bank. The period of concealment was less than a month.

17. Fictitious commercial loans were set up by a branch manager by creating false input documents. New fictitious loans were created eventually to pay off older fictitious loans. In those cases where a demand loan had been created, he paid interest to keep the loan current. The perpetrator input file maintenance changes to ensure that all bank mail pertinent to the fictitious loans would be routed to post office boxes he controlled.

The fraud was discovered by audit confirmation and by a customer's complaint of irregularities at the branch. The auditors investigated loan confirmations returned by borrowers whose addresses were listed as post office boxes. Checking the signatures on the confirmations, the auditors found them to be questionable in comparison with the bank's signature card files. Further communication with the people listed as borrowers uncovered the fraud. The total amount was $120,000. It was concealed for five years, and over 100 transactions were involved.

18. The EDP manager made program alterations causing activity on his account to be suppressed from the detail on overdraft reports although the total was correct. He also made a change to ensure that no statement would be prepared for his account. All of the checking programs were changed to avoid his account. Checks that were paid against his account would be removed from the files before they were filmed. The account became overdrawn, but it was never reported as such. Since no statement was ever prepared, no one became aware of the overdraft in the normal course of operations. In this way, the EDP manager was able to set up a potentially unlimited overdraft line for himself. The fraud was detected by running internal audit software independently against the files. The fraud was concealed for a period of six and one-half years. The total amount of the overdraft accumulated to $40,000 and involved over 100 items.

19. A data entry clerk used a CRT terminal to set up a fraudulent revolving credit line for a check/credit account in his name. The credit line was never

properly authorized. The perpetrator then drew the full amount of the credit line and deposited this amount to his account. Access to the computer terminal was not restricted. Computer reports of the new loans set up were not reviewed.

The total amount of the fraud amounted to $6,000. The period of concealment was five months. It was detected when one of his transactions was rejected due to a systems change (requiring that loan cycle dates and checking statement cycle dates coincide). Investigation found that his credit line was not authorized.

20. An applications programmer-analyst used a vendor-supplied utility program to make two fraudulent transfers from customer savings accounts into his own. The total fraudulently transferred was $10,000. The perpetrator then withdrew the entire $10,000 from his account the next day.

At the time of the fraud, the bank was undergoing a major systems conversion. During this conversion, programmers were allowed to routinely enter the computer room to operate and test programs. Since the bank's savings system was in a conversion mode, the audit department of the bank had been watching exception transaction reports very closely. The bank's daily reporting systems identified large transactions against savings accounts. On this day, the auditors noted a large $10,000 withdrawal from an account that reported a previous day's balance of only $3. They also noted that no $10,000 deposit transaction had been recorded simultaneously. This unusual withdrawal, without an offsetting deposit should have caused an overdraft. Upon investigation, it was determined that the account belonged to an employee of the computer service center.

21. An operations officer in the charge card department would divert customer payments to his own account by keying in his account number on payment processing documents. The perpetrator's duties included investigation of customer complaints. If he received a complaint on one of the defrauded accounts, he entered a payment to that account and debited a suspense account. Suspense debits were lapped to further confuse the trail. After the perpetrator quit the bank, subsequent customer complaints were investigated and led to discovery of the fraud. The fraud was concealed for one year and totalled $3,000.

22. An operations officer increased his own credit line without authority via computer terminal entry. The bank had a terminal system that allowed account information inquiries to be made on-line. Later, a system change allowed for direct terminal update of certain "nonmonetary" fields that included credit line limits. The perpetrator was then able to raise the line of credit on his account and draw the limit. A routine audit test later revealed that this account exceeded its original credit limit. Subsequent investigation found that his unauthorized entry via computer terminal had raised the credit limit. The perpetrator later repaid the loan. The total amount of the line withdrawn was $500, and the fraudulent loan was in effect four months before being detected.

23. A computer operator, using direct access to the master files through a computer console, transferred deposit balances from inactive accounts into accounts controlled by customers with whom he was in collusion. The EDP manager also cooperated in the scheme. The funds were withdrawn from the recipient account by the accomplices. The computer operator hoped to conceal the

frauds by changing the balances during statement preparation. This was to be done by raising the forwarded balance. He chose relatively inactive accounts to further minimize the chance of detection. Finally, he made some unauthorized transfers to accounts owned by persons uninvolved in the scheme to further confuse the situation in case an investigation developed. After a month and a half, however, a customer did complain that his statement balance had been reduced without any transaction being posted. An investigation revealed that the "error" was caused by direct console intervention.

24. An applications programmer, who also functioned as an operator, developed a software program to decrease balances in selected inactive accounts and increase the balance in his own account. No transactions were input, but the files were directly changed. Cycle codes were also altered to ensure that statements would not be mailed until the perpetrator could intercept them. The perpetrator then prepared falsified statements and mailed them to the customers. In one case, the post office returned a falsified statement to the bank, and the perpetrator then didn't bother anymore with preparing statements for the customer. This customer, however, came in and asked for his statement. A subsequent investigation revealed the fraud and identified the perpetrator. The fraud was concealed for a period of 13 months and involved between 11 and 100 items. The total amount misappropriated was $25,000.

Insurance Cases

25. A policy service clerk obtained a management-level password and used it to submit file maintenance transactions to reverse surrendered policies on the master file and to update dividend fields. Policies were later surrendered again and checks made payable to the clerk's spouse. The clerk also manipulated a loan on an active policy, which led to detection of the schemes when the policyholder questioned a loan transaction in response to a confirmation. A follow-up inquiry revealed the improper transactions in the policy adjustment and disbursement areas. The schemes lasted about three months and amounted to $6,000.

26. A policy service supervisor held back incoming cash premium receipts until just prior to the automatic lapsing of policies. "New cash" would then be used to cover the premiums due on the about-to-lapse policies. Sometimes the supervisor used the computer to generate "new cash" by submitting a file maintenance transaction to place the supervisor's name on an active policy that had premiums paid to a certain date. The supervisor would then take an incoming check payment on another policy and apply it to the changed policy; a company check was automatically produced in the supervisor's name with an explanation that the policy was overpaid. A tip from an employee initiated an audit that revealed the scheme. The scheme lasted two years, involved over 100 transactions, and netted $30,000.

27. A policy service clerk had the authority to cross functional department lines to resolve problem cases requiring refunds or return of premiums. The clerk also had authority to initiate and approve disbursement requests. Using these authorities, the clerk initiated fraudulent premium refund requests and

buried the transactions in various suspense accounts. The clerk also submitted override transactions to block automatic adjustments to commissions because of the premium refunds. Detection occurred when the operating management started reviewing old, suspended transactions. The scheme netted $17,000 over thirty-two months.

28. A policy service clerk normally received a computer printout showing the cash surrender values of policies that had lapsed for nonpayment of premiums. The clerk introduced file maintenance transactions to place certain policies back into an active status on the master policy file (always selecting policies with a policyholder name similar to the perpetrator's). The clerk then submitted transactions to produce checks for the policy equity cash value and deposited the checks in an account. The clerk subsequently came forward and revealed the fraudulent activity, which lasted for ten months and amounted to $6,000.

29. To make loan delinquencies appear to be within the established guidelines, a mortgage loan manager used a computer terminal and entered file maintenance transactions to manipulate mortgage loan due dates. Having successfully accomplished this scheme, the manager then began using the terminal to establish fraudulent loans. The total financial manipulation exceeded $320,000, with $55,000 actually converted to cash over a period of nine months. The schemes were uncovered during a routine annual audit.

30. A senior claim processor with signature authority issued claim checks to a fictitious payee that were later forged and deposited in a bank account. To conceal each fraudulent claim check, the processor prepared and sent a data entry code sheet to data processing, which recorded the issued check in the disbursement and statistical claim information files. The processor then destroyed copies of the coding sheets which should have gone into the claim files. The fraud was detected when the processor coded a sheet incorrectly causing a mismatch between the disbursement file and a cancelled check. The fraud lasted sixteen months and exceeded $110,000.

31. In a five-year period, a claim supervisor converted about $500,000 by submitting false health claims that generated checks payable to special payees or outside accomplices covered by group health contracts. The supervisor's position provided access to other people's passwords and negated some of the segregation of duties controls passwords create. In some cases, the supervisor gave fraudulent claim papers to clerks to process in the course of their work and later destroyed the papers. In other cases, the supervisor used a terminal to add names to the eligibility file and then entered fraudulent claim data. Detection occurred when the perpetrator of another fraud told an internal auditor that this might be going on.

32. A group pension supervisor had complete control over payment transactions and related correspondence with contract holders and claimants. The supervisor initiated fraudulent lump-sum payment requests for eighteen months. The computer control to detect duplicate payments was based on a comparison of social security numbers, which the supervisor circumvented by transposing

the social security numbers of the fraudulent payments. The fraud, which exceeded $400,000, was revealed when a legitimate retiree requested a lump-sum benefit and a clerk remembered seeing a previous claim payment to the retiree.

33. A policy service supervisor submitted file maintenance transactions to change the name and address fields on valid master policy record files to those of family members. The supervisor then prepared coded input documents to authorize fictitious premium refunds amounting to over $14,000. Once the computer-generated refunds were made, the perpetrator restored the correct data on the changed policy records. The fraud, which lasted four months, was detected in the bank reconciliation process when a clerk, instructed to review checks for unusual items, noticed a series of large amounts to the same payees and addresses.

34. A producer, working with a policy service clerk as an accomplice, created bogus policies and manipulated valid ones to obtain loans and the full annualized commissions when only one monthly premium was paid. The perpetrators used error correction routines to prevent recovery of the annualized commissions when the bogus policies were cancelled. In addition, fictitious premium "paid-to" date entries were made to increase case equities. The perpetrators then submitted policy loan requests for the increased cash equity and negotiated checks that were made payable to the insured. The schemes lasted five years and netted $300,000. Detection occurred when the producer complained about a commission payment, which aroused a supervisor's suspicion.

35. A policy service supervisor responsible for the dividend unit created fictitious dividend payments by submitting requests with bogus policy numbers; the checks were mailed to an outside accomplice. When the check was authorized by the supervisor, the check data automatically created the accounting entry and simultaneously updated the master policy file. Because a bogus number was involved, an update of the policy file would reject and the transaction would appear on an error report that was returned to the supervisor for investigation. Apparently, these listings were subsequently destroyed by this individual. The scheme was discovered accidentally during a routine review of dividend transactions at the corporate office. It lasted thirty months and netted $150,000.

36. A policy service clerk introduced file maintenance transactions to cancel active policies, which produced policyholder cancellation notices and premium refund checks. The clerk destroyed the cancellation notices and forged the refund checks. The clerk then followed a special error correction procedure to reinstate the policies with full coverage. This scheme was detected through a non-routine study of paid checks in which an employee noticed many out-of-state policyholders had apparently cashed their checks locally. The scheme lasted one year and netted $25,000.

37. A policy change clerk with access to an on-line terminal entered name and address changes to alter the policy master file records to the clerk's spouse. Using general ledger transactions, the clerk caused refund checks to be mailed to the spouse. The refund accounting entry was entered into a general ledger

suspense account not adequately controlled at the time. Detection was made when a supervisor routinely reviewed the suspense account for old items. The scheme netted $5,000 in four months.

38. A group dental claim processor obtained the names of covered employees from a co-conspirator employee of a policyholder company. Using a terminal, the clerk entered fictitious claims made payable to the covered employees, but mailed to a post office box. The checks were obtained, signatures forged, and proceeds ($30,000 in twenty-one months) split. The fraud was detected when the claim clerk was absent and a replacement clerk routinely called a dentist for verification of the nature of a claim.

39. Three claim processors, using terminals, entered fictitious claim data causing computer-produced checks to be sent to each other's home addresses. The supervisor had lunch with one of the perpetrators who mentioned that one of the other perpetrators, now an ex-employee, was being investigated for dental claim frauds by the new employer. The supervisor initiated an audit of the claims processed by the informer and the ex-employee; the audit eventually disclosed the three perpetrators. This scheme lasted for sixteen months and netted $80,000.