Fraudsters, Churches, Economy, and the Expectations Gap: Applying Trends of Occupational Fraud to an Assurance Engagement Team Plan and Fraud-Prevention Client Proposal

by
Jenny Casey Trout

A thesis submitted to the faculty of the University of Mississippi in the partial fulfillment of the requirements of the Patterson School of Accountancy (ACCY 420: Research and Development Series) and Sally McDonnell Barksdale Honors College

Oxford, Mississippi
May 2014

Approved by:

_____
Advisor: Dr. Victoria Dickinson

_____
Committee: Dr. Kendall O. Bowlin

ACKNOWLEDGMENTS

I would first like to thank the following accounting professionals who allowed me to interview them on their perspective of various occupational fraud topics: Mr. Rob King of The Koerber Company, P.A, Ms. Linda Trifone of BKD, LLP, and Mr. Michael Barnes of Johnson Controls, Inc. They provided valuable information on their jobs that helped progress my thesis beyond my expectations. Secondly, I would like to acknowledge the Honors College juniors of the ACCY 420 Fall/Spring Semester class who motivated me and sympathized with me throughout the entire thesis process, especially the late nights spent in the Honors College. I would particularly like to thank Dr. Victoria Dickinson, my advisor and professor of the ACCY 420 class. Without her hard work and advice, my thesis would still be a blank page. Lastly, I would like to recognize my family and friends who have always believed in me when at times, I didn't even believe in myself. It is because of them, I truly know I can conquer the world or, at least, this thesis.

ABSTRACT

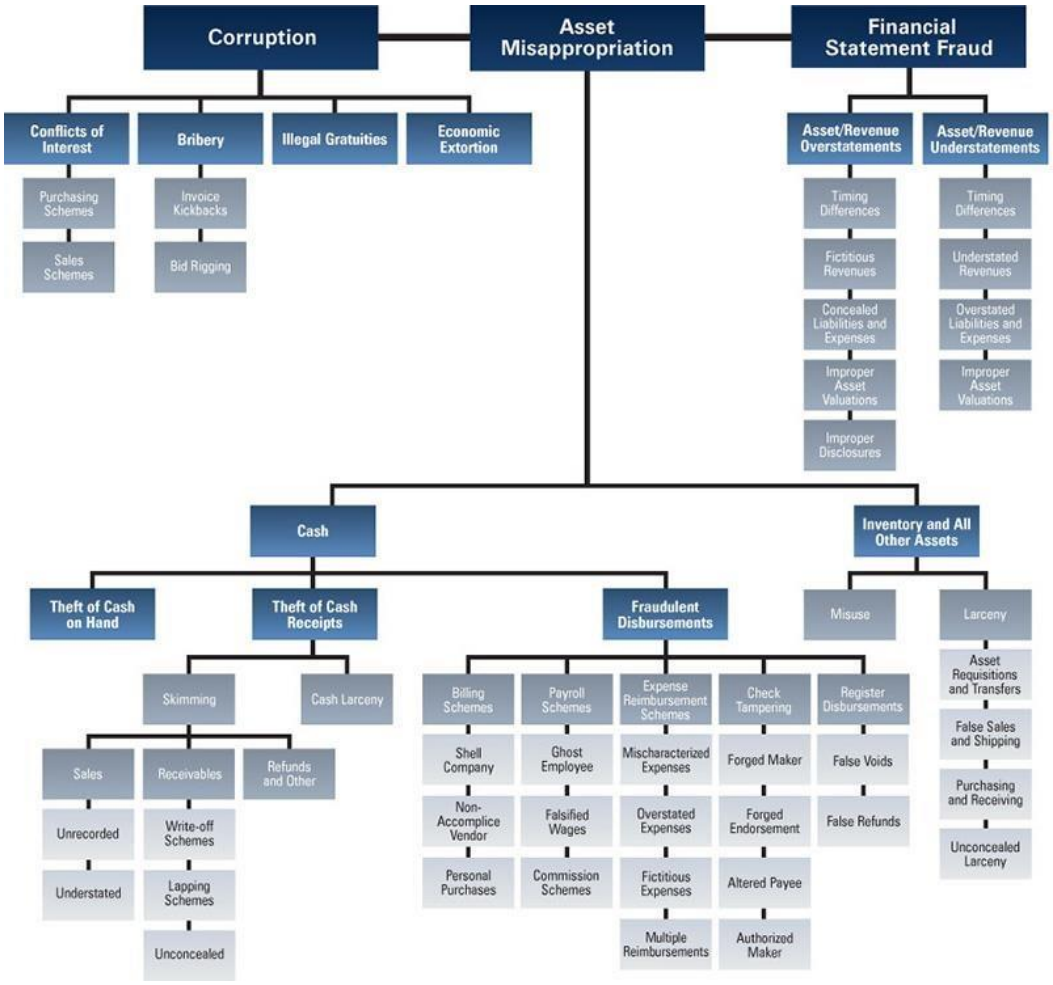
The purpose of this thesis is to present an overview of fraud, including concepts, trends, and controls to in turn, develop an effective assurance work plan as well as a fraud-prevention proposal to a potential client. When KPMG collected data from 348 of their company fraud investigations in 2011, an average of 87 percent were male (3). Around thirty-two percent of fraudsters usually worked in a finance role which gave them access to assets and financial statements. According to Donald Cressy's research, it takes all three elements to be considered fraud: a triangle of motivation, opportunity, and rationalization. However, in the 2004 CPA Journal, David T. Wolfe and Dana R. Hermanson discussed the addition of another element from their research to create a fraud diamond, which also includes the individual's capacity. Compared to public companies, fraud occurs more frequently in privately owned companies. Nearly 40 percent of victim organizations in the Association of Certified Fraud Examiners' 2012 study were privately owned while 28 percent were publicly traded. Furthermore, fraud is more likely to be detected by individuals in the internal or external audit setting or an anonymous tipline. These concepts are explained further in sections of the assurance engagement team plan and fraud-prevention proposal to a small business owner.

TABLE OF CONTENTS

The Expectations Gap for Auditors is driven by two factors: the auditor's aptitude to detect fraud and the auditor's efforts to detect fraud. (Zikmund).When performing an audit for a company, auditors are either inexperienced or not willing to spend the time and energy to perform the steps that stem from the red flags of auditing (Zikmund). To prevent fraud, all accountants, internal or external, must develop fraud detection skills and a mindset to discover fraud. (Zikmund). The purpose of this thesis is to present an overview of fraud, including concepts, trends, and controls to in turn, develop an effective assurance work plan as well as a fraud-prevention proposal to a potential client.

Overview of Fraud

The Association of Certified Fraud Examiners first defined occupational fraud in 2002 as "the use of one's occupation for personal enrichment through deliberate misuse or misapplication of the employing organization's resources or assets" ("Report to the Nations" 2). There are four elements that must be fulfilled to be considered fraud: a material false statement, the employee had knowledge that statement was false, the company relied on the statement, and the company suffered damages because of the activity (Wells 8). There is fine line between fraud and abuse. While abusive practices like surfing the internet while at work and using sick leave when not sick might cause the company to lose resources, they do not constitute fraud (11). Occupational fraud can be divided into three general categories: asset misappropriation, corruption, and fraudulent financial statements, as shown in the fraud tree on the following page.



"Fraud Tree" acfe.com

Asset Misappropriation focuses on theft of cash and the misuse of a company's assets, particularly inventory (Wells 41). If a store employee has been fired and the manager is still reporting their payroll after their termination to pocket the paycheck, this is considered asset misappropriations as a ghost employee. Corruption is caused by wrongful acts in which fraudsters use their influence for a benefit, like bribery, conflict of interest and extortion (41). The Fraudulent Financial Statements category involves misreporting financial statements on purpose to mislead analysts, investors, or creditors (41). Employees can overstate assets/revenue or understate liabilities/expenses in order to make financial statements look more appealing to shareholders or potential investors.

Typical Attributes of a Fraudster

When mentioning white-collar crime like fraud, many accountants and accounting students already have a predefined image in their head of the perpetrator. Big 4 firm, KPMG, describes the typical attributes of fraudsters to be "male, ages 35-46, in a senior management position" ("Profile of a Fraudster" 1). When KPMG collected data from 348 of their company fraud investigations in 2011, an average of 87 percent were male (3). Around thirty-two percent of fraudsters usually worked in a finance role which gave them access to assets and financial statements (4). Fraudsters working in the CEO's office or an operational/sales role were both just under thirty percent (4). Furthermore, over sixty percent of fraudsters worked in senior management position, such as chief executive (4). The Association of Certified Fraud Examiner's Report to the Nations issued in 2012 produced similar results from CFE surveys. Two-thirds of the fraudsters were male and the two highest percentages in age range were 36-40/41-45("Report to Nations" 46). Data differed with the fraudster's position. The position of employee had the highest percentage of fraudulent cases with 41 percent, compared to senior managers and top executives ("Report to Nations" 39). However, the average dollar amount lost from an executive committing fraud in the US was the highest amount at $373,000, almost seven times that of the median loss of employees. ("Report to Nations" 31). While fraud can be man-dominated, women do commit fraud. A global comparison showed that women in the Americas (22 percent) and Asia Pacific (23 percent) are almost three times more likely to be involved in fraud than in Europe (8 percent) ("Profile of a Fraudster" 3). This could be due to fewer European women in top management positions.

Fraud Triangle

While there are common attributes of a fraudster, the situational aspect of fraud is also important. Donald Cressy researched fraud to hypothesize "Trusted persons become trust violators when they conceive of themselves as having a financial problem which is nonshareable and are aware this problem can be secretly resolved by violation of the position of financial trust…" (Wells 13). This conclusion has led to the concept of the fraud triangle: motivation, opportunity, and rationalization (see graphic). Motivation is the perceived nonsharable financial need or "driving force" behind the act (Biegelman and Bartow 33). It is usually caused by greed as described by "living beyond one's means", addiction, family circumstances, or the pressure to pay debts. (33). At times, revenge, ego, or the pressure to perform can play an alternative role instead of greed (33). The second factor is opportunity, which is determined by position of authority and access to resources (34). Fraudsters must have the opportunity to commit fraud as a result of weak internal controls, lack of supervision, and/or poor ethical culture (Dorminey et al.). This is the only element that can be prevented if companies are proactive in their risk management, internal controls, and fraud prevention programs (Biegelman and Bartow 35). Rationalization justifies the fraudulent activity by cognitive reasoning like "I was only borrowing the money; This is not much money so the company won't miss it; I'll stop once I get over this financial hump; The company owes it to me, etc" (35). When fraudsters justify embezzling money by persuading themselves they will pay it back, this payback usually does not occur (Dorminey et al.). Fraudsters rationalize the fraud in order to consider their action acceptable.

Fraud Diamond

According to Cressy's research, it takes all three elements to be considered fraud. However, in the 2004 CPA Journal, David T. Wolfe and Dana R. Hermanson discussed the addition of another element from their research to create a fraud diamond (see graphic below), which also includes the individual's capacity (Dorminey et al.). In previous major scandals, there has been one individual or set of individuals with the right capability, meaning personal traits and abilities that set everything in motion.

The Fraud Triangle

The Fraud Diamond

During a speaking engagement in 2013, WorldCom controller David Myers takes responsibility for his acts involving fraudulent financial statements and journal entries. Yet he also admits that he trusted Chief Financial Officer Scott Sullivan as Sullivan used his capacity to tell Myers and other employees to manipulate journal entries. Myers expected Sullivan to handle any issues if they arose (Myers). In 2005, William Black created the term "control fraud" by studying activities where the CEO or other top executives used the

organization for personal gain (734). He also provided a description for "red-collar" to define white-color criminals who become violent and demanding to their employees as they try to hide their fraudulent actions (734). While red-collar crime and control fraud represent extreme cases of fraud, it still relates to the broad category of the fraud diamond term, capacity.

Magnitudes of Loss

The biggest magnitudes of loss with fraud are related to cost and reputation even though the loss varies with each case. The Association of Certified Fraud Examiners estimates around five percent of all revenue is lost to fraud each year ("Report to Nations" 4). Hypothetically, if a company has a reported net revenue of one million dollars, the ACFE estimate predicts that $50,000 of it is lost to fraud within the company. The median loss based on business size will be discussed further in the 'Trends of Fraud' section as well as a Cost-Benefit Analysis for fraud prevention controls in the client proposal. The size of the fraud can also impact the company stakeholders' opinion. If the company cannot recover their financial losses, employees might be laid off. Investors will evaluate whether or not they should continue doing business with the company. Lastly, the consequences from the fraud—i.e., employees let go, bad publicity--could change customers' view. Even if the company recovers from the fraud financially, the consumer's negative opinion of the company image and reputation could affect the business continuity.

Punishments

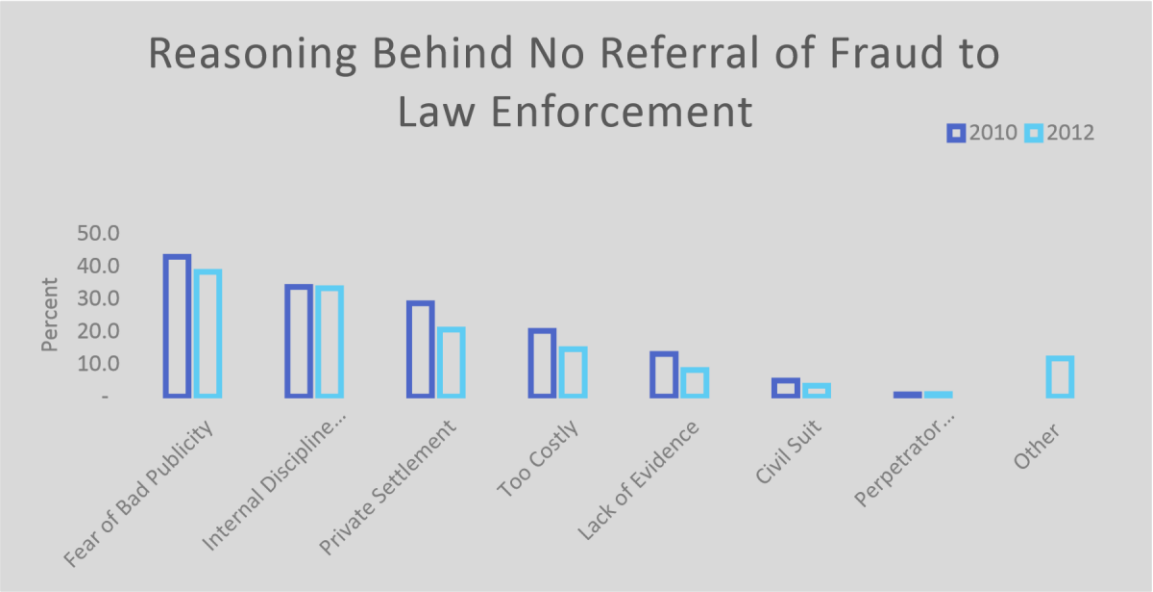
Most fraudsters who are caught will have their punishments determined by the company, based on the notion if they decide to pursue legal actions. To summarize the punishments exacted on fraudsters presented in the 2012 Report to the Nations, around 65.4 percent of fraud investigations are handed over to police (61). When Sarbanes-Oxley was implemented, it created and amended specific statutes fraudsters are faced with if their cases are prosecuted (Biegelman and Bartow 75). Convictions of certain activities like "Destruction, Alternation, or Falsification of Records in Federal Investigations and Bankruptcy" result in a fine, up to 20 years imprisonment, or both (75). The Securities Fraud statute provides penalties of a fine and/or imprisonment of a maximum of 25 years if a criminal is convicted of defrauding public company shareholders (75). The following table presents a comparison of convictions of two highly-publicized scandals versus a smaller scandal. However, it should be noted that they are roughly eleven years apart.

Company	**WorldCom**	**Tyco**	**RH Holdings(Southhaven, MS)**
Year	2002	2002	2013
Fraud Amount/Type	$3.8 billion dollars Financial Statement Fraud	$600 million Securities Fraud	$5 Million Dollar Loan Credit Application Fraud
CEO Conviction	Bernie Ebbers convicted to 25 years in jail	Dennis Kozlowski served 8.7 years in a sentence up to 25 years	Contractor James Harris convicted to 21 months in prison and $247,467 in restitution
CFO/Partner Conviction	Steve Sullivan convicted to 5 years in jail Controller David Myers convicted to 1 year and 1 day	Mark Schwartz served 8.4 years in a sentence up to 25 years- Total both paid $104 million in restitution and $105 million in fines	Partner Chuck Roberts served 10 days in prison for crime
Source	The Executive Roadmap	The Executive Roadmap	http://www.desototimes.com (3/29/14)

As the table shows, even ten years ago, a fraud worth several hundred millions or even billons resulted in several years of jail time. CEO Bernie Ebbers is currently still serving

his 25 year sentence. In a small Mississippi town, Harris was convicted to almost two years of jail time for a fraud of 5 million dollars.

Alternatively, in 2012, 34.8 percent of fraud was not referred to law enforcement as listed in the 2012 Report to Nations (61). As shown in the graph below, companies do not often report fraud because they fear bad publicity toward the company or the company feels their disciplinary actions are sufficient (61)



"Reason(s) Case Not Referred to Law Enforcement ", 2012 Report to Nations, Association of Certified Fraud Examiners

However, because of their reasoning, fraudsters are getting the chance to potentially continue their crime at another business. According to the 2014 PwC Global Economic Crime Survey, approximately eighty percent of fraudsters were dismissed from the company, yet only forty-nine percent were reported to law enforcement (49). Many fraudsters are essentially allowed to walk free. Since they were not prosecuted, nothing shows up on a pre-employment background check and they are able to continue their tactics at a new company.

Fraud in Private Companies versus Public Companies

Compared to public companies, fraud occurs more frequently in privately owned companies. Nearly 40 percent of victim organizations in ACFE 2012 study were privately owned while 28 percent were publicly traded ("Report to Nations" 25). Because private companies are not regulated by the Securities and Exchange Commission, they have fewer protocols to follow and do not have the internal controls public companies do. Private companies focus primarily on the profitability and financial standing of their business. The Banking and Financial Services, Government and Public Administration, Manufacturing, Healthcare, and Education industries are the top five industries most susceptible to fraud ("Report to Nations" 28). Since these industries require a high proportion of financial reporting and accounting as well as a large number of employees, it is understandable they have the most cases of frauds.

Fraud in Non-Profit Organizations

While most fraud occurs in for-profit industries, there are some occurrences in the nonprofit sector. Around ten percent of fraud cases have been investigated in non-profit organizations, compared to a combined approximate of seventy percent in for-profit industries ("Report to Nations" 25). Theft of cash and kickbacks/bribery were the most common types of fraud committed in non-profit organizations with the most non-profit frauds occurring in organizations with very few volunteers (Buckhoff and Parham 54). With no volunteers, officials committing fraud can easily hide their actions as they do not have to worry about many people examining the non-profit finances.

Fraud in Churches

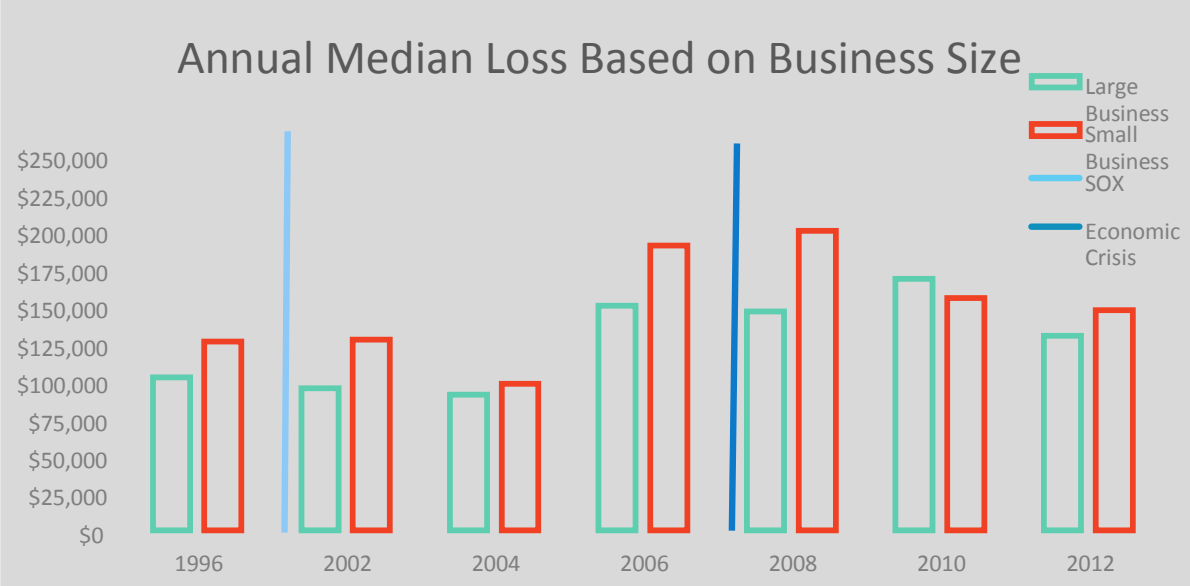
Magnifying the non-profit sector, churches actually lose a large amount of money to fraud each year. The Status of Global Mission's 2014 Report concluded that around the world, an estimated 39 billion dollars is budgeted annually for ecclesiastical crime, which is considered money embezzled by top custodians of religious money (29). Perpetrators use their personal relationships with fellow believers in the church to partake in dishonest activities. Since churches typically give all their proceeds to religious activities and missions, very little time or money is spent on internal controls. This makes it easier for fraudsters to gain the trust of church officials as well as gain access to the church offering or finances to use for their personal expense. While churches publish their financial statements and budgets to inform the congregation, churches are not required to be audited by accountants. Additionally, churches are usually tax-exempt so the IRS only audits if they have a notion of illegal activity ("Tax Information for Churches and Religious Organizations").

Trends of Fraud

Tracing Fraud over Time

Since many fraud occurrences are not detected or not turned into legal investigations, the rise or decline of fraud cases over time is not clear. According to the Report of Nations surveys from 1996 to 2012, fraud has been exposed as either five or six percent of yearly revenue. In PwC's Global Economic Crime Survey for 2014, their research concluded the reported rate of economic crime around the world had increased from thirty percent in 2009 to thirty-seven percent in 2014 (5). In 2011, the rate was from the report was in the middle at thirty-four percent (5). Though, by surveying Certified

Fraud Examiners each year, data does show annual trends pertaining to specific details of fraud. As shown in the graph below, the median loss of small businesses versus large businesses has fluctuated since 1996. The average loss decreased until 2006, when it increased significantly.



"Size of Victim Organization — Median Loss", Report to the Nations, ACFE, 1996-2012

The light blue line on the graphs notes the creation of the Sarbanes-Oxley Act in July, 2002, which could have had an effect on the decrease of fraud loss. Additionally, the dark blue line depicts the Economic Crisis in 2008. The median loss of fraud increased significantly around this time when companies and individuals were struggling financially.

Economy's Effect on Fraud

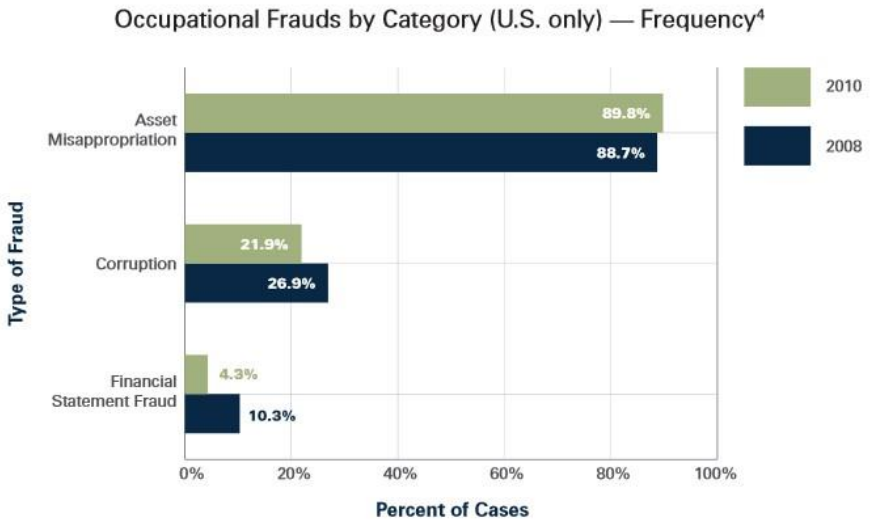
Furthermore, this data can predict that the trends of fraud are affected by the general economy. Shown by the dark blue line on the graph, the economic crisis of 2008, including the housing bubble and economic recession, impacted fraud heavily. An additional ACFE

survey tested this theory as they received responses in February and March 2009 from 507 Certified Fraud Examiners. Ninety-two examiners found a significant increase in fraud and 189 examiners discovered a slight increase ("Occupational Fraud" 5). The average dollar amount of fraud also increased by almost 49 percent (5). During the recession, aside from living beyond one's means and financial difficulties, businesses were also faced with the pressure to succeed despite the poor economic circumstances. The recession study found that of the frauds detected at around this time, forty-nine percent happened because of increased pressure. ("Occupational Fraud" 6). ACFE President James D. Ratley reiterated this by stating "Desperate people do desperate things." (14). Companies must reduce expenses to maintain revenue and since internal controls "do not contribute to the bottom line", they can be one of the first expenses to be decreased. (14).

"Types of Fraud Observed to Have Increased During Past Year," Occupational Fraud: A Study of the Impact of Economic Recession

However, data conflicted when researching the change in the three types of fraud during the Economic Crisis. The ACFE survey about the Recession showed that all types

of fraud increased significantly in the time between 2008 and 2009 as in the graph above (9). Yet when comparing the percent changes of the ACFE Report to the Nations from 2008 to 2010 (next page), none of the categories showed dramatic increases. In fact, two types, corruption and financial statement fraud, decreased in percentage. Taking the survey details into account, this could have been caused by the difference in sample sizes and sample respondents.



"Occupational Frauds by Category (U.S. only), Report to the Nations, 2010, Association of Certified Fraud Examiners

Media's Effect on Fraud

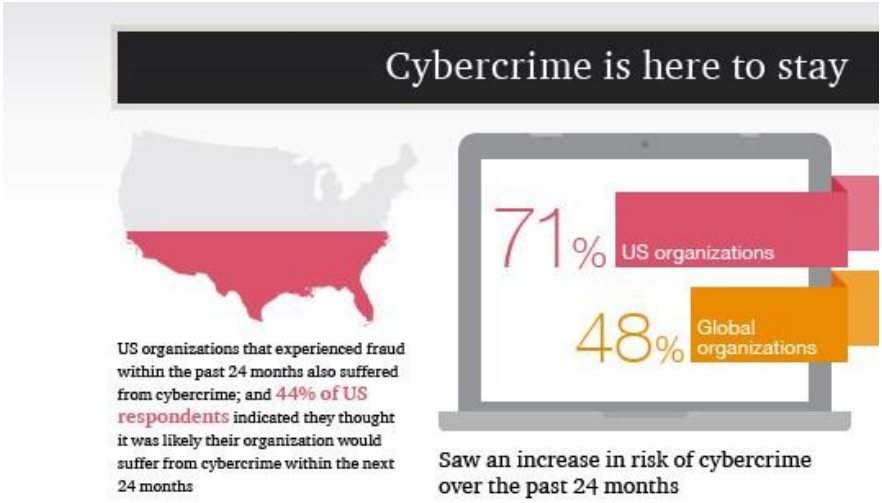
Media has little impact on actual fraud but has more influence on informing the public after it has been detected and investigated. Unless journalists are given insider tips, they have no way of knowing fraud was occurring in the company until it was publicly announced. Once details of the fraud are released to the public, news stations can then report on it. Media is also impacted by the size of the fraud relative to the company. Most U.S. adults could probably name top frauds that have occurred in the past ten years just

based on media attention. Publicly traded Fortune 500 companies receive more commerce than small-town businesses; therefore, the public is more likely to be interested in the public companies when fraud occurs.

Social media could play a large role in detecting fraudulent activity by providing evidence on the activities of a fraudster. If a tip is turned in about an employee's possible theft of company money to fuel a gambling addiction or management notices an employee living beyond their means, websites like Facebook and Twitter can indicate if he or she has visited a casino or store recently through pictures, statuses, and check-ins. Postings can even be traced to geographic coordinates if the settings are turned on. While it might be difficult to prove the crime completely off of social media, it could provide helpful evidence towards the fraud case.

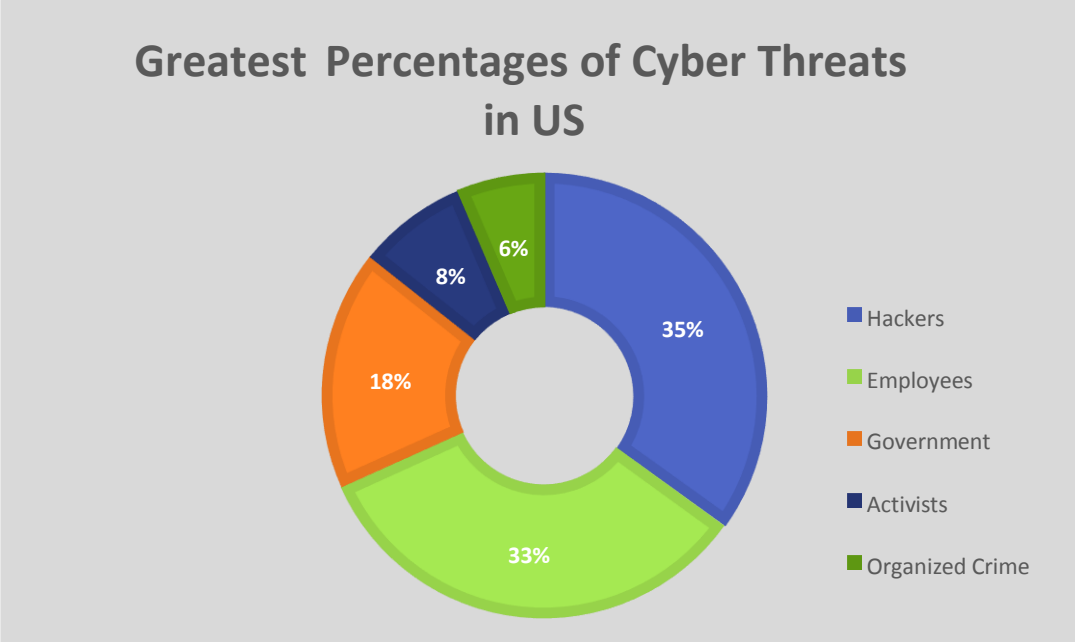
Cyber-Fraud

Cyber-crime has a three point definition; therefore, each point represents a separate concept. The first part of the definition includes cyber-fraud and describes as "traditional crime like fraud or forgery carried out over electronic communication networks and information systems" ("European Commission"). The second part of cybercrime is related to illegal activity over the electronic media like child pornography as well the third section which details crimes against networks like hacking or attacking an information system ("European Commission"). While each point is a different way to commit crime, they are usually grouped together under the phrase cyber-crime. As technological activities increase exponentially, cyber-crime is also increasing as shown in the graphic below.



"Global Economic Crime Survey", PwC, 2014

Nearly all companies conduct business using technology and the internet. Trends of cloud computing, mobile technology, data mining, and video conferencing are quickly infiltrating into the business world. Technology has impacted the accounting profession as a large majority of businesses use Accounting Information Systems and Enterprise Resource Planning system, like SAP and Oracle, to automate accounting processes. As technology expands further into the business world, new issues, specifically in the area of intellectual property, arise. Robert King is a CPA, CVA, and CFE at the consulting firm, The Koerber Company, in Hattiesburg, MS, which specializes in forensic accounting and litigation. Based on his experiences, he has realized that this is becoming a big issue because IT officials can relocate from one company to another and steal a company's proprietary information for their own benefit (King). Since companies survive by doing things better than their competitor, any theft, especially intellectual property, could seriously impact finances.



"US State of Cybercrime", PwC, 2013

While increased technology has provided more ways to commit fraud, the main perpetrators of cybercrime are disgruntled employees, hackers, and the government as shown in the graph on the previous page. A small percent of sources also include activists and organized crime.

With automated AISs, companies can enact general and application controls for technology. If a company does not have these controls in place, they have a higher chance that fraud will be committed. If company networks do not have both physical and logical security measures, it can be very easy for someone without authority to gain access to tangible assets like inventory and intangible assets through the Accounting Information System. However, implementing controls specific to risk areas in the company can affect the occurrence of fraud.

Cybersecurity Initiatives

As cyber-crime rises, the government has taken action to help prevent cybercrime. In the past few months, the Obama Administration issued a "Framework for Improving Critical Infrastructure Cybersecurity" for nationwide security. This executive order sets guidelines for organizations to manage cybersecurity risks by focusing on risk assessments and response plans (Exec. Order No. 13636). Furthermore, the FBI has established multiple task forces to help alleviate cybercrime like the National Cyber Investigative Joint Task Force. This special force teams up with nineteen other intelligence agencies to help detect cybercrime and the major culprits behind it, which are discussed in the section below ("National Cyber Investigative Joint Task Force")

Social Demographics

Looking at the Federal Bureau of Investigation Cyber's Most Wanted list, it should be noted that of the ten individuals on the list, most of them have similar demographics. All individuals were males and a majority were young adults ("Cyber's Most Wanted"). Nine out of the ten were born in between 1970 and 1990 and most had some background in computer programming, telecommunications, or internet entrepreneurship ("Cyber's Most Wanted"). The ten most wanted represent a variety of European and Middle Eastern nationalities. Additionally, as with the Cyber's Most Wanted, most cybercrime occurs in urban areas because cybercriminals have more network access there.

Undetected Fraud

When fraud goes undetected for a long period of time and is then found, specific aspects of the business could really be in trouble. Fraud could seriously impact business continuity depending on the level of financial stability of the company. Significant financial losses due to fraud and fees resulting from the fraud could hurt company to the point of bankruptcy or acquisitions. When reporting for undetected fraud on the financial statements, a prior period adjustment could cover small amounts of fraud and disclose in the footnotes depending on the level of materiality. If the fraud will impact the financial statements considerably, they would need to reissue all prior financial statements for the years fraudulent activity occurred. A product of the Sarbanes-Oxley Act, Public Company Accounting Oversight Board committee might also get involved with the audit and assess not only the company, but the external audit team responsible as well. If the fraud was detected early and the company needed to report a net loss for the year, they could partake in a deferred tax carryback or carryforward. However, if the fraud is detected too late, they might not have this opportunity. Public perception of the company could also be damaged if the fraud goes undetected for a long period of time. Customers could view it as irresponsible and decrease their loyalty to the company. Competitors could use it to market to lost customers. Many times businesses do not prosecute detected fraud once found in order to save reputation and prevent bad publicity.

Combating Fraud

There are three main types of controls in accounting: external controls, internal controls, and codes of ethics. Each type attempts to control and prevent fraud as well as errors in a different way by either regulations inside or outside of the company.

External Controls

The biggest external control that has affected the entire accounting world is the formation and implementation of the Sarbanes-Oxley Act (SOX) in 2002. President George W. Bush signed it on July 30, 2002 and stated, "Every corporate official who has chosen to commit a crime can expect to face their consequences" (Biegelman and Bartow 68). It reinforces corporate accountability by promoting auditor independence as auditors must rotate every 5 years and auditors are prohibited from offering any non-audit services to the company (69). SOX also created the Public Company Accounting Oversight Board, which inspects public accounting firms and the audit process for their respective companies (69). In addition to strengthening the independence of audit committees, Sarbanes-Oxley requires company executives, like CEO and CFO, to verify and certify financial statements (69). While it is hard to tell definitively if the number of fraud cases has been reduced since SOX was recognized, it has established more structured rules and guidelines in hopes of preventing fraud in the future.

The Statement of Auditing Standards (SAS) 99 also provided a turning point for external controls involving fraud. SAS 99 gives external auditors the "responsibility to plan and perform an audit to test whether financial statements are free of material misstatements caused by error or fraud" (Biegelman and Bartow 82). The standard focuses on planning/performing an audit by having brainstorming sessions and analytical reviews to induce skepticism about fraud or errors and identify fraud risks. When external auditors

find evidence of fraud, they must then report it to top management or the audit committee, if the fraud involves top executives (Biegelman and Barlow 89).

Additionally, several task forces have been created to help investigate and prevent major fraud from occurring. During the same month Sarbanes-Oxley was passed, Bush started the Corporate Fraud Task Force (Biegelman and Bartow 19). This task force was responsible for not only investigating all the major fraud scandals like Enron, Rite Aid, and Adelphia, they also were in charge of prosecuting them. When Barak Obama became the United States President, he replaced the Corporate Fraud Task Force with the Financial Fraud Enforcement Task Force (Biegelman and Bartow 20). This new task force stresses the investigation and future prevention of fraud caused by the economic crisis in 2008 (20). Likewise, the Securities and Exchange Commission started a similar task force, the Financial Reporting and Audit Task Force, in 2013 to help regulate financial reporting by public companies (Novack). Their main priority is to start a RoboCop initiative using the new Accounting Quality Model (AQM) to test the risk involved with earnings management. Craig Lewis, Chief Economist and Director of the Division of Risk, Strategy, and Financial Innovation ("RSFI") at the SEC, discussed that the RoboCop will be able to detect when a company has high book earnings with an alternative tax treatment or a high number of transactions that took place off the balance sheet (Novack). While the RoboCop program has flaws, like its reliance on financial comparisons between companies in the same industry, the RSFI is trying to improve upon it by incorporating word tests into the AQM as well. Looking at a past fraudulent filings, RSFI analysts have developed lists of words and phrasing choices which have been common amongst fraudulent filers and turned into one of the elements in the AQM test (Novack). The automated process starts the day after public companies turn their financial statements into Edgar (Novack). The

RoboCop tests the statements against the AQM and a risk score is created, which is then analyzed by the SEC to determine if the score is high or low on a scale of fraudulence (Novack). External controls, such as laws and task forces, provide general rules and guidelines for all companies to follow.

Internal Controls

While external controls set a foundation for rules and guidelines, internal controls are implemented within the company for its own benefit with risk management. There are three types of internal controls that focus on efficiency and effectiveness: preventative, detective, and corrective. Before implementing internal controls, companies should identify and evaluate the risks to their most valuable processes by doing an assessment. Each company will focus on protecting the core processes. A retail store will have inventory controls in place to protect their inventory and other assets. A corporation with large data collections will have security controls, like locked computer storage facilities, biometrics, and passwords. Similarly, a company who uses an Enterprise Resource Planning system will give each employee an account with a strong password and access limited to what their scope of work relies on.

Internal Audit

Having an internal audit department that is a separate subsystem from the accounting department is an important function to internal controls for a company. They perform operational audits to evaluate financials and operations independently of what the rest of the company is reporting. The CFO decides what the internal audit team should focus on annually, based on what has been audited in the past year and what the external

audit team is concentrating on (Golden et al. 165). While an internal audit team can investigate fraud if it is detected, there is a point they must hand the investigation off to consultants or specialists if it reaches beyond their scope (166).

Codes of Ethics

SOX also emphasized ethical values, as each company is now required to have code of ethics for senior officials (Biegelman and Bartow 74). The Code of Ethics is separate from a company's mission statement, but the two could be harmonious. Walmart's Statement of Ethics for all employees includes a specific clause for financial reporting:

> *"Walmart requires honest and accurate recording and reporting of financial information in order to make responsible business decisions. All financial books, records, and accounts must accurately reflect financial transactions and events. They must conform to generally accepted accounting principles, and to Walmart's system of internal controls" ("Statement of Ethics").*

Despite the fact Walmart has global operations, all employees in all countries, from Chief Financial Officer to a cashier dealing with cash transactions, must adhere to the Statement of Ethics. Having a company-wide code of ethics provides ethical guidelines if an employee's integrity is in question.

Publicly-traded manufacturer and service provider, Johnson Controls, Inc, also has a similar section in their code of ethics: *"We ensure our books and records are accurate, complete and maintained according to the law and industry best practices"* (Roell, 22).

Michael Barnes, Accounting Manager at the Johnson Controls plant location in Hattiesburg, Mississippi, agrees that while ethics policies provide a good base point to establish internal controls, they do not directly contribute to fraud prevention ("Ethics at Johnson Controls"). If a fraudster has the motivation and opportunity, they will find a way to bypass the controls, regardless of the ethics policy in place. The ethics policy also relates to the concept of tone-at-the-top, which expects senior executives and management to be models for all other employees. In his interview, Mr. Barnes also notes that tone-at-the top in the control environment is very accurate as having good control leadership and the policies in place go hand-in-hand ("Ethics at Johnson Controls"). Aside from ethical codes, companies also must have whistleblower protection as described in Section 806 in Sarbanes-Oxley (Biegelman and Bartow 263). Additionally, in 2010, the Dodd-Frank Act was passed to give whistleblowers compensation for their relevant information (263).

Assurance Opportunities with Fraud Investigation

Difference between External Auditors and Forensic Accountants

External Auditors and Forensic Accountants both work to detect and investigate material fraud, but each have their own view of the task. In this analogy, an auditor could be compared to a policeman and a forensic accountant investigator to a detective (Golden et al. 22). An audit team analyzes financial statements for a company they have a contract with. In their audit plan, they have specific steps to take to test for risk of fraud. A forensic accountant usually is certified as Certified Fraud Examiner. They could work for either a public firm in the Forensic and Fraud Services branch or for a consulting firm. They specialize in fraud investigations and putting in controls to prevent future fraud risks. This topic is further explained in the Work Plan subsection later on in this section.

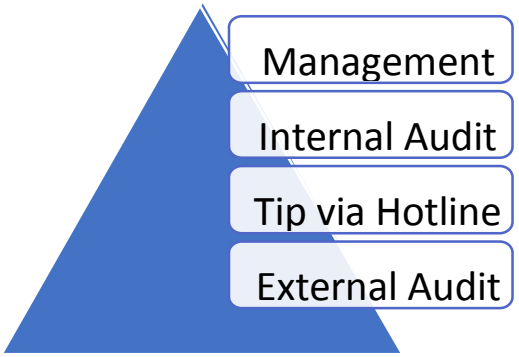
Fraud Investigations vary in cost on a case-by-case basis. Linda Trifone, Director at BKD, LLP and Certified Fraud Examiner, gives an example of an actual case that had fraud dating back 36 months and involved around $500,000 in stolen funds from the fraud (Trifone). The accounting and legal costs to investigate were over $100,000 (Trifone). At a consulting firm, the typical costs for services around $3,500 to 12,000 based on billable hours (King). For fraud cases, a retainer is used to collect fees upfront (King). Cost can be a deterrent for a fraud investigation and will be discussed later on in the Work Plan section.

Impact of Big Data on Fraud Investigation

Since more and more companies are collecting data and storing it in data warehouses and data marts, fraud investigators have additional data to work with when analyzing a fraud. The concept of big data is no longer a phenomenon but a reality that can be used to prevent and investigate data for fraud. Investigators can use data mining to efficiently look for suspicious findings by sorting and querying different scenarios like "Round-Dollar Payments" and "Gaps, Voids, and Canceled Checks" in a database (Golden et al. 408). Data-mining accounts for Benford's Law, which is the notion that fraudsters typically use a figure that begin with the number 9. This goes against the assumption that the higher the number is, such as 7, 8, or 9, the less probable it will be the first digit value in an amount (Biegelman and Bartow 319). Additionally, as more data is collected and analyzed, more information goes into the ERP. This can help investigators if they need to do a search instead of having to search through gigabytes of unstructured data.

Work Plan for Engagement Team

The beginning steps of a fraud investigation are determined by the detection method. If top management detects it, executives are already aware of what has happened. From there, they can proceed quickly with how they want to investigate the issue. If an internal audit detects it first, they must first bring the issue to management, who then decides how it is handled. This scenario started the WorldCom investigation, even though management played a role in the financial statement fraud. While tip hotlines are the largest way to detect, truthfulness is an issue. The reports can be anonymous and anyone with access to the hotline can report so it could be a more lengthy process to test the accuracy and truth to each fraud claim. However, the tip could be a stepping stone for further investigation if it proves to be correct.



A typical engagement team includes a partner who assumes final responsibility, a manager, an industry specialist, and a number of senior, associate, and intern staff members (Robertson and Louwers 88). An interim engagement budget in terms of hours could be 160 hours with a year-end engagement budget that increases to 175 hours (88). Internal Control evaluation during the interim is budgeted to be around thirty hours and planning the engagement to be twenty-five hours total (88). It is during this time that the team conducts risk assessments for possible fraudulent activity. If fraud is detected at any time during the engagement, the scope would shift from a financial statement audit to a fraud investigation. The engagement team could bring in a specialist with fraud investigation experience, usually a CFE with independence from the company being

audited to make the investigation objective. This individual helps lead the team with the partner and to teach inexperienced staff how to investigate fraud.

If fraud is found but it is not during an external audit, the executives can decide how they want to proceed. If they believe the fraud may have a major impact, they can call in a specialized team of fraud investigators, usually certified fraud examiners, using a consulting firm who focuses on forensic accounting. They could also employ a Fraud and Forensic Services team from a public accounting firm who they are not contracted with for audit services. Sarbanes-Oxley prohibits firms from performing audit and non-audit services for the same company.

Once the investigation starts, the first steps should be gaining an understanding and gathering information and documents about the case (Golden et al 299). The engagement team must then decide how to proceed with document review, identifying witnesses, and holding interviews. The team must make arrangements if outside legal counsel is requested.

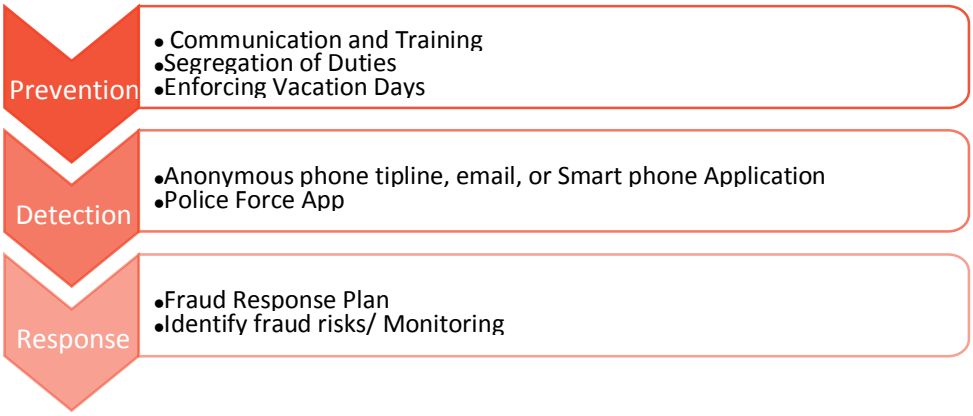
However, since a fraud investigation can be very costly, the company could proceed using internal audit if they were just looking for enough evidence to terminate the employee committing fraud (Trifone). Prosecution makes the investigation much more costly and in the end, the outcome of investigation might be unfavorable to the company.

Client Fraud-Prevention Proposal

(Note: In this section, my team is presenting to a small business, a service provider, with less than 100 employees. A majority of the employees work within the office headquarters. It is assumed there is an owner, a general manager, and two assistant managers who share responsibility of the company.)

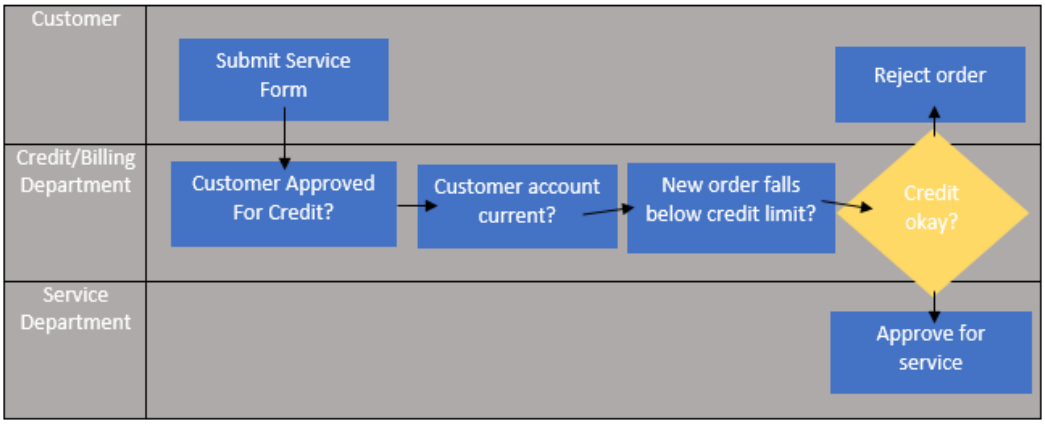
For small businesses, the focus is on creating a successful and profitable company, so having a large variety of expensive internal controls and risk management processes is not feasible. Yet the lack of controls could lead to fraud. According to the ACFE's Report to Nations, businesses with less than 100 employees are the most common victims of fraud (26). While data is skewed by the CFE report because few small businesses hire CFEs to investigate the fraud, their research does show in 2012 that 31.8 percent of fraud cases occurred in small businesses (26). This percent is up one percent from 2010 (26). Small businesses were more susceptible to billing schemes, check tampering, skimming, and expense reimbursements than larger companies with over one hundred employees (27).

After analyzing the company, we found that it is in the small business' best interest to invest in a fraud prevention program that they find is cost-effective to their net income. Below is our proposal to a potential client, a small business owner, of the benefits of having minimal internal controls to help prevent fraud. To lower costs, business owners could focus on one main control for each category: prevention, detection, and response. Below are considerations of basic internal controls that small businesses would benefit from.



Preventative Measures

For prevention, our first suggestion would be planning and compiling policies, procedures, and all other guidelines into a Company Handbook distributed to each new employee starting at the company. Written procedures aid in training new staff on business processes quickly. Newly-added procedures and controls could be communicated to veteran employees via continuous training session presentations or informal material could be distributed through a company memo. The guidelines and policies should reiterate the company's zero-fraud tolerance and state the punishment exacted on the fraudster if caught. Secondly, the company should be structured (or restructured) to include segregation of duties. This control helps avoid giving employees control of an entire process. Essentially, one employee's work serves as a check for another employee. Management should assign tasks like authorizing transactions, recording transactions, and maintaining custody of the assets to at least three different employees. The graphic describes a second-level process map for the credit approval process for a customer wanting the services offered by the company. Since it is a small company, owners should keep a map of the processes with notes on what steps each employee or department is responsible for.

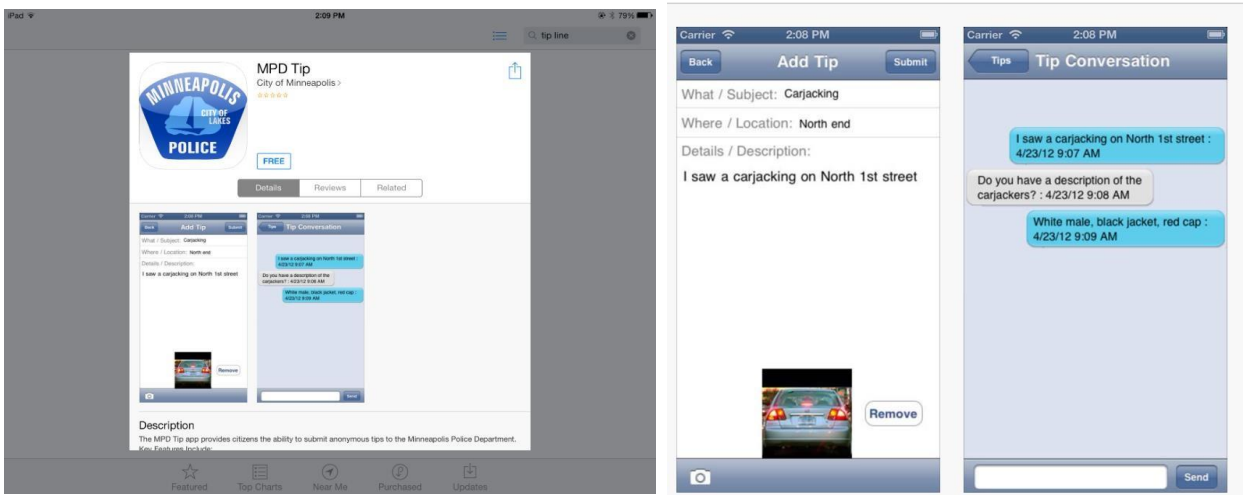


The owner and general manager should also mandate vacation days in the company policies. One of the behavioral red flags of fraudsters is their refusal to take vacations (Report to Nations, 2010). They know if they leave the company for a short amount of time, their fraudulent activity could be detected. Mandatory vacation days would rotate the job tasks to another employee or manager for a few days and fraud risks or even fraudulent evidence could possibly be detected.

Detective Measures

In terms of detection of fraud, a method that has proven to be effective is the use of anonymous hotlines/tiplines. Research has shown employees and others reporting fraud like the anonymity and confidentiality it brings (Golden et al. 26). In 2012, tips were the largest way to initially detect occupational fraud in any industry with a percent of around 43 percent, compared to management review (14 percent) and internal audit(14 percent) (Report to Nations 14). Over fifty percent of tips were reported through employees but it should be mentioned that twelve percent of tips were anonymously reported. Additionally, tips were best reported with organizations that had hotlines at 51 percent versus those that didn't offer hotlines at 34.6 percent (17).This proves that using a tipline could increase management's knowledge and detection of ethical misbehavior/complaints and potentially decrease fraud occurrences. Various companies specialize in their hotline services but the cost of the services is based on a price estimate because of customization. A basic hotline provider like AnswerNet or Fraud Hotline costs around $500 to 1140 dollars annually for a small business of 100 employees (Andrews and LeBlanc.). The medium hotline service providers such as Red Flag Reporting and Lighthouse services charge a minimum of $645 to 800 dollars for a company with 100 employees (Andrews and LeBlanc).

A possible suggestion would be a tipline through a smartphone or computer application instead of a telephone system. With technology increasing, people might be more susceptible to report fraud if they can use their mobile phone or tablet. Little research has been conducted for this idea but the average cost of developing an application with lower-level complexity and a small feature list is around 50,000 dollars (SAP). An example of a police department app that has similar features is below. Developers could link the application to the AIS the company uses or have each report sent directly to management or internal audit.



MPD Tip Cell Phone Application, City of Minneapolis

If a company is not collecting enough profits to have an anonymous hotline internal control, management should still make it understood in the policies and procedures handbook what to do to report a claim. The company could set up an additional phone number or email address just for reports or the company could direct employees to utilize local police department resources like CrimeStoppers hotline or the smart phone application posted above by the City of Minneapolis Police Department.

Every company, no matter the size, should also have a fraud response plan. Preventative programs will not stop all fraud so a company should have a plan of action in place if fraudulent activity is detected. (Golden et al. 233). Below are components of the sample fraud policy found on the BKD website:

REPORTING PROCEDURES	Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way. An employee who discovers or suspects fraudulent activity will *contact the* _____ *Unit immediately*. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the Investigations Unit or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: "I am not at liberty to discuss this matter." *Under no circumstances* should any reference be made to "the allegation," "the crime," "the fraud," "the forgery," "the misappropriation," or any other specific reference.
TERMINATION	If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from Human Resources and the Legal Department and, if necessary, by outside counsel, before any such action is taken. The _____ Unit does not have the authority to terminate an employee. The decision to terminate an employee is made by the employee's management. Should the _____ Unit believe the management decision inappropriate for the facts presented, the facts will be presented to executive level management for a decision.

By including this information in the employee handbook, all employees will be aware of the actions and consequences faced with committing fraud. The manager and owner should also frequently spend a significant amount of time assessing controls for fraud risk and monitoring all activities. Since it is a small company, management could try to actively review each employee's behavior for any red flags as well as verify finances and

operations. By evaluating and monitoring specifically for fraud, management will be able to detect correct weak internal controls that could lead to fraudulent activity.

Cost-Benefit Analysis

In our proposal, we present to a small business who is privately owned and less than 100 employees. Unfortunately, a company of this type does not publicly release their financial statements. We have used the actual financial information from ARAMARK Corporation in September 2006 when they employed 240,000 individuals (Hoover 53). ARAMARK is a private company that provides food services and uniform services. ARAMARK provides the food services for the campus of the University of Mississippi, Individually, the ARAMARK services offered to the University of Mississippi could be comparable to a small business. In 2006, ARAMARK's total revenue was 11,621 million dollars (Hoover 53). Using the ACFE estimate of five percent revenue lost to fraud each year, ARAMARK would lose $581,050 of their 2006 revenue. Below in Cost-Benefit Analysis to reflect the results by implementing a fraud prevention program as described in the proposal. It should be noted that the three percent and five percent savings are hypothetical and not proven to be probable. The amount expensed for 2006 is also hypothetical and includes the cost of the fraud prevention program if executed.

Benefits	**Costs**
No Fraud Prevention Program- No Savings	**Revenue 11,621,000**
	Less: Estimated Revenue Lost to Fraud 581,050
Profit Margin 5.76%	**Actual Revenue 11,039,950**
	Expenses 5,000,000
	Net Income 6,360,000
	Cost Ratio 44%

Benefits	**Costs**
Fraud Prevention Program- 3% Savings	**Revenue 11,621,000**
	Less: Estimated Revenue Lost to Fraud(2%) 232,420
	Actual Revenue 11,388,580
Program cost of $1000 expensed	**Expenses 5,01,000**
	Net Income 6,388,580
	Cost Ratio 43.9%

Benefits	**Costs**
Fraud Prevention Program- 5% Savings- No Fraud	**Revenue 11,621,000**
	Less: Estimated Revenue Lost to Fraud 0
	Actual Revenue 11,621,000
Program cost of $1000 expensed	**Expenses 5,000,000**
	Net Income 6,621,000
	Cost Ratio 43.1%

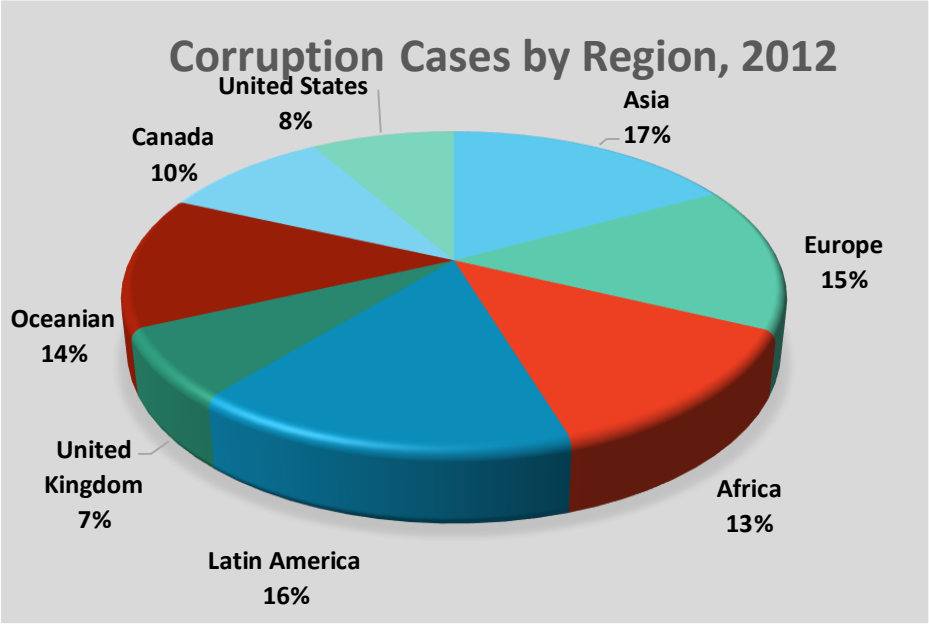
By implementing a fraud-prevention program, the analysis shows the comparison of expenses to net revenue estimated by the amount lost by fraud decreases by almost one percent. As the company grows and revenue increases, they can put more money into the prevention program if needed or develop the smart phone application.

Anti-Fraud Initiatives

Global Fraud and Initiatives

Every country deals with the element of fraud and its consequences. Using the Gross Domestic Product(GDP) of the United Kingdom, fraud in the public sector is estimated to be around $20.6 billion per year(“Annual Fraud Indicator” 8). The UK has also taken measures through the National Fraud Initiative to help track down fraud as well

as the implementation of the UK Bribery Act in 2006 ("National Fraud Initiative). The NFI helped trace 275 million dollars' worth of fraudulent activity in 2010(National Fraud Initiative). The graph below displays how the US compares to other countries based on the number of corruption cases the ACFE analyzed.



"Corruption Cases by Region", Report to Nations,2012, Association of Certified Fraud Examiners

Compared to the UK GDP amount, the United States GDP, with five percent of revenue lost to fraud as mentioned earlier, the present value US GDP from 2013($16,799.7 billion) would include $839 million lost to fraud. While the United States has struggled significantly with fraud, it does indicate that we have fewer corruption cases than other regions.

Conclusion

In order for auditors to be able to successfully detect fraud during an engagement, they must be well informed on all aspects of occupational fraud. Studying and analyzing concepts like attributes of fraudsters, trends of fraud, cybercrime, and fraud prevention programs could close the Expectations Gap between auditors. In turn, this knowledge can help plan better for the logistical measures and processes of an engagement team who might have to conduct a fraud investigation.

References

Andrews, Christine P., and Brian P. LeBlanc. "Fraud Hotlines: Don't Miss That Call." *Journal of Accountancy* (2013): n. p. Aug. 2013. Web. 9 Apr. 2013.

Annual Fraud Indicator. Rep. National Fraud Authority, June 2013. Web. 10 Apr. 2014.

Barnes, Michael. "Ethics at Johnson Controls"" E-mail interview. 7 Apr. 2014.

Biegelman, Martin T., and Joel T. Bartow. *Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance*. Hoboken, NJ: Wiley, 2012. Print.

"Sample Fraud Policy." BKD, LLP, n.d. Web. 16 Apr. 2014.

Black, William K. "“Control Frauds” as Financial Super-predators: How “pathogens” Make Financial Markets Inefficient." *The Journal of Socio-Economics* 34.6 (2005): 734-55. *Science Direct*. Web. 10 Apr. 2014

Buckhoff, Thomas, and Abbie Gail Parham. "Fraud In The NON Profit Sector? You Bet." *Strategic Finance* 90.12 (2009): 53-56. *Business Source Complete*. Web. 4 Apr. 2014.

"Cyber's Most Wanted." *FBI*. FBI, 08 May 2013. Web. 08 Apr. 2014.

Dorminey, Jack W., Aaron Scott Fleming, Mary-Jo Kranacher, and Richard A. Riley, Jr. "Beyond the Fraud Triangle." *The CPA Journal* 80.7 (2010): 17-23,3. *ProQuest.* Web. 4 Apr. 2014.

European Commission. *Towards a General Policy on the Fight against Cyber Crime*. European Parliament, 2007.

Exec. Order No. 13636, 3 C.F.R. (2014). Print.

Fraud Tree. Digital image. *Acfe.com*. Association of Certified Fraud Examiners, n.d. Web.

Global Economic Crime Survey. Rep. PriceWaterhouseCoopers, 2014. Web. 3 Apr. 2014.

Golden, Thomas W., Steven L. Skalak, and Mona M. Clayton. *A Guide to Forensic Accounting Investigation*. Hoboken, NJ: J. Wiley, 2006. Print.

Hoover's Handbook of Private Companies, 2008. Austin, TX: Hoover's Business, 2008. Print.

King, Robert. E-mail Interview. 14 Apr 2014.

Myers, David. "Faith and Practice." Christ Church Winnetka., Winnetka, IL. 8 September 2013. Keynote Address. Found on www.youtube.com

"National Cyber Investigative Joint Task Force." *FBI*. FBI, 21 May 2010. Web. 13 Apr. 2014.

"National Fraud Initiative." *Audit Commission*. 2012. Web. 17 Apr. 2014.

Novack, Janet. "How the SEC's New Robocop Profiles Companies for Accounting Fraud." *Forbes*. N.p., 9 Aug. 2013. Web. 4 Apr. 2014.

Occupational Fraud: A Study of the Impact of an Economic Recession. Rep. Association of Certified Fraud Examiners, 2009. Web. 1 Apr. 2014

Profile of a Fraudster. Rep. KPMG, 2011. Web. 1 Apr. 2014.

Report to Nations. Rep. Association of Certified Fraud Examiners, 2012. Web. 3 Apr. 2014.

Robertson, Jack C., and Timothy J. Louwers. *Auditing*. Boston: Irwin/McGraw-Hill, 1999. Print.

Roell, Steve. "Ethics Policy." *Johnson Controls*. 1 Jan. 2011. Web. 4 Apr. 2014.

"Statement of Ethics." *Walmart.com*. N.p., n.d. Web. 4 Apr. 2014.

"Status of Global Mission." *International Bulletin of Missionary Research* 38.1 (2014): 29. Web. 1 Apr. 2014.

"Tax Information for Churches and Religious Organizations." *Internal Revenue Service*. Web. 11 Apr. 2014.

Trifone, Linda. Email Interview. 15 Apr 2014.

Wells, Joseph T. *Principles of Fraud Examination*. Hoboken, NJ: John Wiley, 2005. Print.

Zikmund, Paul E. "Reducing the Expectations Gap." *The CPA Journal* (2008). Web. 3 Apr. 2014.