HOW HAVE CHANGES IN TECHNOLOGY IMPACTED THE ABILITY TO COMMIT AND DETECT FRAUD, AND HOW SHOULD THE ACCOUNTING WORLD RESPOND?

by

Sarah James

Submitted in partial fulfillment of the

requirements for Departmental Honors in

the Department of Accounting

Texas Christian University

Fort Worth, Texas

May 2, 2016

HOW HAVE CHANGES IN TECHNOLOGY IMPACTED THE ABILITY TO COMMIT AND DETECT FRAUD, AND HOW SHOULD THE ACCOUNTING WORLD RESPOND?

Project Approved:

Supervising Professor: Chad Proell, Ph.D.

Department of Accounting

Stacy Grau, Ph.D.

Department of Marketing

ABSTRACT

Fraud is not a new topic. However, with the inclusion of technology into the workplace, criminals have a new means of engaging in fraudulent activity. Currently, the accounting world has two fraud detection mechanisms: the financial audit and the fraud audit. The fraud audit is specifically designed to catch fraud and ignores materiality thresholds. Despite being the most successful detection mechanism, it is currently not required for publicly traded companies. Though the accounting world could simply mandate the performance of a fraud audit, the added costs associated with performing the audit could cause smaller businesses to suffer and would likely be met with significant pushback from the business community as a whole. Therefore, it is highly unlikely that the fraud audit will be mandated in the near future. Thus, the financial audit will remain the primary method of fraud detection. Currently, the financial audit focuses on material misstatements, which may or may not be related to fraud. With a significant portion of frauds going undetected, the financial audit's ability to detect fraud must be improved. One method to improve the financial audit's fraud detection rate is to improve the ability the auditors, to detect fraud. This paper discusses how technology has impacted the ability to commit fraud and in turn how these changes have impacted the ability to detect fraud. As well as discusses improving the ability of the financial auditor to detect fraud via improvements in their training, specifically accounting curricula, can help compensate for the impacts technology has had. Changes to accounting curricula would consist of incorporating forensic accounting and deception detection courses in order to enable students to better understand the various elements of fraud, improve their ability to recognize fraud, and improve their professional skepticism. Such improvements will increase the ability of the financial auditor to detect fraud, and by extension improve the ability of the financial audit to detect fraudulent activity.

TABLE OF CONTENTS

INTRODUCTION

It is somewhat impossible to be engaged in the realm of accounting, or business for that matter, and not have heard about the Enron scandal. The Enron fraud was one of the largest accounting scandals of the late 1990s. As such, it caught the attention of both law enforcement and the accounting world, increasing the focus on fraud prevention. The scale of this fraud, as well as others of the time period such as WorldCom, and Tyco, led to several changes in legislation. The most notable change being the passage of Sarbanes Oxley in 2002. All of these legislative changes had the intent of preventing fraud. Despite these changes however, each of the "Big 4" CPA firms when surveyed said they expected fraud to increase (Hays & Ariail, 2013). Fraud is an issue the accounting world, and law enforcement, have been concerned with for decades and unfortunately it is an issue professionals view as increasing in prevalence. Though it is not a new topic, it is important to recognize that the increasing presence of technology in the work force has significantly changed fraud, and as a result the way it should be handled. In the past, financial fraud was committed by obtaining access to physical papers or devices. In today's society as businesses have started to rely on and incorporate technology to improve efficiency a new avenue for fraud has been created, making it easier than ever to engage in fraudulent activity (Guillot, 2013).

Unfortunately, the way technology has impacted fraud has made current detection measures insufficient. The main tool currently used to fight financial fraud is the financial audit. Many companies have come to rely on the financial audit as a means to detect and deter fraud. However, there is a large gap between what regulators and investors expect the financial audit to accomplish and what it is actually required to accomplish. Many believe that the financial audit is designed to catch all fraud. In truth, the financial audit is designed to catch material misstatements

which may or may not be related to fraud. The auditor performing the financial audit evaluates the financial statements through sample based testing, then he/she provides an opinion on the financial statements as a whole as to whether or not the statements are reasonably presented and free of material misstatement (Albrecht & Hoopes 2014).

Now the question is, if we are detecting material misstatement why should the accounting community care? Currently, the financial audit only detects 10 percent of financial fraud (Singleton & Singleton, 2007). Now even if the financial audit is catching all material misstatements, including those related to fraud, then when this 10 percent success rate is considered, it means 90 percent of frauds are operating under materiality thresholds. Additionally, such a low detection rate means that the majority of criminals engaged in fraudulent activity are going undetected. This low detection rate, is one of the possible reasons fraud has continued to grow in prevalence because fraud perpetrators believe they can get away with committing and concealing the crime. Improving the ability of the financial audit to detect non-material fraud will benefit the community in several ways, including: preventing businesses from losing funds to fraud and enabling them to reinvest those funds and further emphasize the fact that fraud is a criminal act and it will be prosecuted at all levels.

One of the main tools that auditors use when evaluating fraud is the fraud triangle. The fraud triangle consists of three parts: Opportunities, Attitudes/Rationalization, and Incentives/Pressures. The fraud triangle involves looking at fraud from the perpetrator's standpoint (Buchholz, 2012). The fraud triangle is used in the audit planning process "to make sure those potential fraud risks are identified and are examined to ensure that those potential fraud risks are not present and have resulted in a material misstatement on the financial statements" (Buchholz,

2012, p.110). The fraud triangle is an extremely valuable tool in detecting material misstatement (Buchholz, 2012).

However, the inclusion of technology into the workplace has changed the weights of the fraud triangle making opportunity greater than ever, thereby increasing the ability of the perpetrator to rationalize the act (Guillot, 2013). With the increased opportunity and ease of rationalization, it reduces the importance of the criminal having an incentive. Think of it this way, if you ask anyone if they want more money, they are going to say yes. Therefore, if a perpetrator can easily gain access to the company's assets without getting caught and can justify the act in his/her mind, then they don't need much of an incentive to commit the crime. In short, technology has altered the way perpetrators approach fraud and therefore the accounting world should change its approach as well.

Currently, there is one option the accounting world has at its disposal that could catch fraud, despite the impact that technology has had. This tool is known as the fraud audit. The fraud audit is an extremely effective mechanism used by accountants to detect and investigate fraud; it is designed specifically to detect fraud within an organization and encompasses an evaluation of accounting information systems (Singleton, 2007). While many companies may potentially opt to use the fraud audit as an added measure of prevention, it is currently not required for publicly traded or private companies.

Although the fraud audit has been proven to be effective, there are some drawbacks to implementing it. The fraud audit is an added expense that many companies are not willing to undertake (Albrecht & Hoopes, 2014). Additionally, if an individual in a position of power within the organization is guilty of committing fraud, it is highly unlikely that he/she would incorporate a measure that would increase the likelihood of being caught. This fact, combined with the added

costs companies would face implementing a fraud audit, make it a rather unlikely tool for the accounting world.

As the financial audit is currently the only audit that public companies are required to undergo, and consequently the main method of fraud detection, then auditors are the soldiers in the fight against fraud. They are on the front lines so to speak. Therefore, if the accounting world is to adapt the way it approaches fraud in order to improve the chances of detecting it, it is my opinion that the start should not be with legislation. I say this for two reasons: 1) changes in legislation have already been made and fraud continues to be a growing issue and 2) although mandating the fraud audit would be a simple solution to the growing fraud problem, there are other avenues that can be pursued that would incur less pushback from the business community. If the accounting world were to mandate the fraud audit, smaller firms might not have the funds to incorporate the change and it could cause smaller businesses to suffer. Additionally, larger corporations would see this accounting change as a decrease to profits. If other avenues exist that would not outrage the business community, then those should be pursued first.

One such avenue would be to start with those directly involved in the fight, the auditors. More specifically, the accounting world should work with Universities to incorporate certain changes into accounting curricula that would improve the auditor's chances of detecting fraud, and in turn improve the effectiveness of the financial audit. Many researchers have already keyed in on the fact that there needs to be a greater focus on forensic accounting in accounting curricula, as it better helps auditors understand fraud and the various ways that it can be perpetrated (Daniels et al, 2013). While I agree wholeheartedly, I think that improvements in accounting curricula should extend beyond just the incorporation of forensic accounting and should include classes on deception detection. These deception classes would give auditors the ability to pick up on verbal

and non-verbal cues of deception and enable them to expand their professional skepticism to interactions with the client. These classes could greatly improve the auditor's ability to detect fraud, as individuals engaged in fraudulent activity often use forgery and lying to conceal their crimes. Additionally, there are often individuals who are aware of the fraud, but who are afraid to disclose what they know (Albrecht & Hoopes, 2013). Including deception detection courses would enable the auditor to analyze and detect human elements of deception, thus allowing them to detect factors the financial audit is not currently designed to. Such an improvement in the auditor's abilities will consequently improve the audit's effectiveness in detecting fraud. Though the inclusion of deception courses may seem like something available only to government agencies, and therefore not a feasible option, access to these courses, which include the analysis of micro expressions, speech patterns, and verbal cues are available already to the general public. Therefore, implementation of deception detection classes at the University level would be a feasible option.

LITERATURE REVIEW

What is Fraud?

Fraud takes many different forms, each unique but all with one uniting factor, deception. Financial fraud is defined as:

> An intentional act committed by one or more individuals among management, other employees, those charged with governance, or third parties. Financial fraud involves the use of deception to obtain an unjust or illegal advantage. These activities can include misappropriation of cash or inventory, fraudulent financial reporting, and money laundering" (Newman, 2009, pp. 72-73).

The misappropriation of cash and inventory can take two paths. If these activities occur before the transaction is recorded, then they are referred to as skimming activities (Lord 2010). Think of it like this: your mother gives you money to go to the store and you get $20.00 in change, however you decided to take $5.00 for yourself as payment for the task and tell your mother that you only received $15.00 dollars in change. In other words, you skim a little bit off the top.

If, however, the misappropriation of cash and inventory occur after the transaction is recorded, then it is referred to as larceny, or theft (Lord 2010). Consider the example given earlier, instead of your mother giving you money to go to the store for her, she brings you with her. You see that she receives $20.00 and you feel that you are owed something for the trip. When she is not looking you take $5.00 out of her purse. It may not seem like a big deal at the time, but whether it is $5.00 or $5,000,000 it is still considered fraud and it is still a crime.

The definition of fraud provided previously highlights another category of fraud called fraudulent disbursements. Fraudulent disbursements are essentially false disbursements that relate to cash or other assets leaving the company as a form of payment (Lord 2010). Consider the grocery store example used earlier. Instead of being the child accompanied by his/her mother, you are now the store clerk making minimum wage. In addition to your Tetris style bagging skills you have been able to access the store's payment system and create an additional employee account, a fake one, which results in you receiving an additional paycheck each payment period. Essentially, the company is paying you twice when it thinks it is paying two different employees. Another example of a fraudulent disbursement would be if you, the store clerk, were to ring up extra items and bill the customer for more than what they were actually getting and pocket the difference. In essence, fraudulent disbursements encompass a wide range of activities including customer billing activities, payroll activities, and other types of thefts (Lord 2010).

Unfortunately, to many individuals the aforementioned examples may not seem like that big of a deal. After all what is $5.00 compared to millions in revenue. But the truth is even the tiniest of frauds add up and negatively impact the business world. In 2008, the Association of Certified Fraud Examiners issued a report that stated in the U.S. alone, organizations were losing roughly 7% of their revenue, roughly $994 billion, to fraudulent activity (ACFE 2008 & Ramamoorti 2008).

The Fraud Triangle

The fraud triangle is a valuable tool used by auditors and organizations to evaluate the risk of fraud and help combat the growing fraud epidemic (Buchholz 2012). The fraud triangle consists of three parts: Opportunities, Attitudes/Rationalization, and Incentives/Pressures (Buchholz 2012). The three elements of the fraud triangle are used to evaluate the risk of fraud by understanding the conditions under which fraud is more likely to occur.

The incentives/pressures element of the fraud triangle relates to the perpetrator wanting to increase his/her economic benefits. Incentives is a broad term that can encompass a variety of factors including: pressure from management, current economic conditions (a recession for example), the need for more income to take care of a sick relative, or more often than not, greed (Buchholz 2012). In other words, incentives get the perpetrator thinking about the fraud to obtain a desired end goal.

Incentives are not the only thing that could interest a perpetrator in committing fraud. Depending of the structure of a business, the opportunity to commit fraud might simply be too great to pass up. This introduces the second segment of the fraud triangle, opportunity. The opportunity segment is exactly what it sounds like; how easy is it for the perpetrator to gain access to the desired information and how easy it is for him/her to conceal the act. Many organizations

tend to focus on this segment of the fraud triangle, as it is the most readily controllable and identifiable element (Cressey 1973 & Singleton et al. 2006). One way organizations combat opportunity is by implementing internal controls. However, though these internal controls may help, they are not without weaknesses, and criminals continue to expose and exploit those weaknesses to their benefit (Buchholz 2012).

Returning to the grocery store example from earlier. Some people might not think that taking $5.00 is a big deal. This plays into the third and final element of the fraud triangle, rationalization/attitude. Many individuals who engage in fraudulent activity feel as though "the actions they perform are not really considered fraudulent as they were entitled since management really owed it for all the years of hard work and service" (Buchholz, 2012, p.112). In other words, the rationalization factor of the fraud triangle revolves around the perpetrator's ability to justify his/her criminal act. This attempt by perpetrators to justify their actions can also extend to include reasoning such as everyone else is getting rich, I'm just borrowing, and it's not like there are any victims (Ramamoorti 2008).

Each element of the fraud triangle, especially the rationalization element, plays into the perpetrator's ability to reduce his/her own cognitive dissonance and feel better about the crime he/she is committing (Ramamoorti 2008). Cognitive dissonance is defined by researchers "as a contradictory feeling a person's mind or the discomfort that arises when a person simultaneously holds two conflicting thoughts" and it is only natural for humans to want to alleviate this discomfort however they can (Yu-Lun and Ching-Jui, 2014, p. 980 & Festinger & Carlsmith 1959).

Consider the example from earlier where your mother gives you cash to go to the store for her. The cashier gives you $20.00 in change and you decided to take $5.00 for yourself. The incentive could be that you want to pick up a candy bar on the way home. The opportunity is that

your mother is not around so there is nothing stopping you from pocketing the $5.00 for yourself, and the rationalization is that you are owed something for running an errand for your mother. Each element of the fraud triangle is present, despite the fraud functioning on such a small scale.

It is evident that the fraud triangle is a valuable tool in evaluating the minds of fraud perpetrators. If a company can understand where the opportunity is stemming from and can work to eliminate that opportunity, then it is reasonable to conclude that the company can reduce its risk of fraud. However, the recent changes in technology have significantly impacted the fraud triangle and its effectiveness. Companies, as well as auditors, must fully understand these changes if they are to respond accordingly (Pearson & Singleton 2008).

The Role of Technology in the Workplace

The rapid inclusion of computers in the workplace has created an entirely new avenue through which individuals can engage in fraudulent activity. Previously, when an individual wanted to commit fraud, he/she had to obtain physical signatures in order to gain access to the desired assets (Guillot, 2013). However, nowadays with more information being kept on computers, perpetrators can bypass management/coworkers and access the assets/funds on their own.

One of the most impactful changes technology has had on the business world is the introduction and incorporation of cloud computing. Cloud computing is currently used in a variety of business processes. Cloud computing, as defined by the National Institute of Standards and Technology (NIST), is:

> a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal

> management effort or service provider interaction (Alali & Yeh, 2012, 14: Jansen and Grance 2011, 11).

Cloud computing has many advantages that continue to draw in users in the professional environment. These advantages include: a reduction of capital expenditures (KPMG 2010), the ability to tie costs to revenues as they are incurred, flexibility (Armbrust et al. 2010), and the ability to reduce the risk of wasting resources (Alali & Yeh 2012). Realizing these advantages, it is no surprise that companies are incorporating cloud computing at an increasing rate. In fact, the prevalence of cloud computing in the business environment has extended to the accounting sector, creating what is now known as cloud based accounting.

Cloud based accounting allows businesses to maintain "centralized accounting data in the cloud [and] leads to more current data for all users and also makes the system more available to office workers, satellite offices, work-from-home employees, sales reps on the road, and even customers (through customer portals)" (Collins, 2015, 107). While this sounds great in theory, many CPA's continue to push back on the utilizing cloud based technologies for accounting purposes, as they believe it is irresponsible to house accounting data in such a way. Yet business organizations continue to be proponents of the cloud based accounting due to the aforementioned benefits, such as flexibility and reduced costs (Collins 2015).

Additionally, some proponents of cloud based accounting believe it to be more secure than desktop and paper accounting. The main argument here is that with desktop or paper accounting, the servers or filling cabinets are in the building, specifically in a room where perpetrators could easily gain access to them simply by breaking in (Collins 2015). Alternatively, when using cloud based accounting the information is stored in "world-class data centers with fortified concrete

walls, steel doors, retina scans…and world-class firewalls, state-of-the-art anti-virus technology, and continuous backups" (Collins, 2015, 107).

While data centers where information is stored are perhaps more secure than a locked filing cabinet or server under the desk, in the sense that someone can't just pick it up and take it, these centers still have security risks. Even companies and proponents of cloud based accounting that realize adopting these technologies can increase the risk of fraud, they may not fully understand how to compensate for the increased risk. With these technologies, criminals no longer have to gain access to the physical documents. They won't need to break into the data system, rather they just need to gain access to certain accounts which usually only requires a password. In fact, researchers have found "that most attacks occur when a fraudster obtains a password to a system" (Guillot, 2013, 46).

To try and combat the ability of criminals to use technology to their advantage, companies have made several strides in protecting data stored on information systems. For example, most accounting information systems have some sort of encryption to protect the data held within them (Collins 2015). Now, while this is incredibly important, I do believe it is more useful to deterring individuals outside of the company from manipulating the company's assets, than it is in deterring employees, especially employees working in the accounting department. The truth is, the biggest security threat/weakness facing a company is its people. In many cases, rather than trying to break into or manipulate computer networks or systems protected by various controls, criminals "prefer to compromise the people who configure, use, and manage them" (Ramamoorti, 2008, 528). Therefore, because people are easier to deceive than computers, an individual looking to engage in fraud could get close to a coworker who has the access they desire and easily "hack" them, acquire the needed password, and commit the crime (Ramamoorti 2008). Additionally, when using

a stolen password, the system would recognize the entry of the password and conclude it is the original owner, not the thief, thus helping the perpetrator to conceal his/her crime. In fact, "white collar crime is notoriously difficult to prosecute because the offenders are well connected and often are first-time offenders. Such fraud perpetrators take extreme care to conceal their activities, destroy evidence, and disrupt the audit trail" (Ramamoorti, 2008, 526). The sheer presence of technology drastically increases the opportunity for individuals to engage in fraudulent activity, because it creates a new avenue via which fraudsters are less likely to be caught.

A real life example of fraud that used the method described above is presented in a discussion with Paul Zikmund, the Director of Global Ethics and Compliance for Bunge Ltd.. Zikmund actually uncovered an embezzlement that occurred when a perpetrator gained access to a manager's password. Zikmund declared that:

> The fraud was enabled by the growing use of technology to improve efficiency. Under the old system, bookkeepers had to submit a form to a manager for vendor approval. But new automation of the process allowed them to create the vendor online themselves and wait for one-click approval. With a manager's password, it was easy to approve the phony vendor (Guillot, 2013, 45).

Though the fraud was caught, it was already three years underway and the perpetrators embezzled roughly $130,000. This example of fraudulent activity highlights one of the biggest risks facing companies that are increasing the presence of technology in the office, which is the ability to verify the authenticity of documents. As Zikmund points out, it is simply much more difficult to judge authenticity when reviewing electronic files. As a result of the inclusion of technology in the workplace, the opportunity for fraud, and the perception that it can be committed and concealed

successfully has increased. Thus making it easier than ever to engage in fraudulent activity (Guillot 2013).

How Technology Has Impacted the Fraud Triangle

A key component of opportunity is that the perpetrator believes that the likelihood of being caught, and subsequently punished, is very low (Ramamoorti 2008). With the incorporation of computers into the work place, criminals are able to engage in fraudulent activity with a significantly lower chance of being caught, due to that fact that computers rarely create the documents needed to aid organizations in identifying fraudulent activity (Pearson & Singleton 2008). An additional means by which technology has aided those engaging in fraudulent activity, is that when organizations implement internal controls, managers typically do not pay enough attention to IT related risks, often due to a lack of understanding, further increasing the opportunity for fraud (Wallace et al, 2004; Kumar 2002; Osmundson et al. 2003).

In addition to impacting the way fraud is committed, changes in technology have also created new avenues to detect fraud. One such avenue being Big Data Analytics. However, one key constraint of Big Data Analytics is that companies have to understand what data to look at and single it out from all the data available. This step is necessary to ensure that the benefits are outweighing the costs. Yet, even if management understands that technology has increased opportunity, and consequently the risk of fraud occurring, they may not fully understand the risks it is facing from an IT perspective. Thus, the beginning stage of singling out data can be extremely challenging. Though challenging, it is still possible. However, there are other deterrents when it comes to Big Data usage. When a company begins to implement Big Data Analytics it needs to have the right team, including data scientists and subject matter experts (Jaeger, 2014). For some companies this could require bringing in an outside team, which would mean additional costs for

a company. Though larger corporations have the resources to implement Big Data and the required teams, smaller organizations might not. Thus, for the purpose of this paper, the financial audit will continue to be the focus, as it is the only detection method that both large and small corporations currently implement.

By making it easier to engage in fraudulent activity, as well as conceal it, technology has also made it easier for perpetrators to rationalize the crime. The rationalization segment of the fraud triangle does not just include the aforementioned reasoning such as *I deserve this* or *I'll pay it back*. Rationalization can encompass anything that the perpetrator can think of that would justify the act in his/her mind, which can include *I'll never get caught* (Verschoor 2015). In short, the less likely the perpetrator believes the chances of he/she getting caught is the more likely he/she is to engage in fraudulent activity.

Though technology has had a less direct impact on incentives, its impact can be seen through the following line of reasoning. Previously, incentive/pressures was defined as a want by the perpetrator to obtain some sort of economic benefit (Buchholz 2012). However, it is not just limited to that, incentives are anything that gets the perpetrator thinking about the fraud. With regard to technology, the sheer ability to commit a fraud and the ease of access to information creates a situation where it is more likely for an individual to consider committing fraud than they otherwise would. Furthermore, the increased ease with which the perpetrator can commit, conceal, and rationalize the fraud decreases the importance of incentives in the fraud triangle. Consider this, if given the opportunity to have more money, the majority of people are going to take it. In short, the ability to commit fraud with ease and get away with it, as made possible by technology, could serve as an incentive.

Current Detection Measures

As a result of the aforementioned impact technology has had on the fraud triangle and business environment, fraud will continue to be an issue. The accounting world has recognized the increasing prevalence of fraud and has taken measures to combat the growing epidemic. The passage of the Sarbanes-Oxley (SOX) Act in 2002 was one such measure. SOX placed stricter controls over the audit process, as well as increased the focus on a company's internal controls, requiring auditors to review their effectiveness (Patterson and Smith, 2007). Internal controls are meant to hinder the opportunity segment of the fraud triangle and reduce the risk of fraud. However, despite the improvements that SOX has fostered when it comes to internal controls, these controls still have weaknesses that criminals have, and will continue to exploit (Bucholz 2012).

The main fraud detection method currently in place is the financial audit. However, it is important to remember that the financial audit, and in turn the auditor, are focused on catching material misstatements, which may or may not be related to fraud (Albrecht & Hoopes 2014). The Generally Accepted Auditing Standards (GAAS) guide the financial audit. The standards of field work, in other words the conduction of the audit, are:

1) The auditor must adequately plan the work and must properly supervise any assistants.
2) The auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures.

3) The auditor must obtain sufficient appropriate audit evidence by performing audit procedures to afford a reasonable basis for an opinion regarding the financial statements under audit. (AU § 150.02)

In addition to being hindered from detecting fraud by the design of the financial audit, financial auditors face the challenge of perpetrators using third parties to conceal their crimes, forgery and lying, and the fear people have of disclosing fraudulent activity they are aware of (Albrecht & Hoopes, 2014). At the end of the day, financial auditors only detect about 10 percent of financial fraud (Singleton & Singleton, 2007). If the financial audit is detecting all the material misstatement, including those related to fraud, then that means 90 percent of frauds are operating below the materiality threshold. This is an issue for three reasons. First, the frauds that occur below the materiality threshold can go on for years, resulting in an end sum that would have been considered material. Secondly, with the fraud detection rate being so low, it increases the perception that an individual can get away with committing fraud, once again increasing the perception of opportunity and the ability to rationalize the act. Finally, such a low detection rate means there is a significant amount of criminals who are not being brought to justice. Therefore, it is imperative that we improve the ability of the financial audit to detect fraud occurring at all levels. Doing so will not only decrease the perception that fraud can be committed successfully, but it will also decrease the amount of funds that businesses lose to fraud.

There is another option besides the financial audit that could improve fraud detection rates. Many people don't know that there is another type of audit specifically designed to detect fraud. This audit has appropriately been named the fraud audit. The reason many people don't know of its existence is that they think it is part of the financial statement audit required for public companies. Unfortunately, it is not. It is entirely separate (Albrecht and Hoopes, 2014). The fraud

audit is actually "much more detailed [than financial audits] and look[s] in greater depth at specific elements that might be misstated" (Albrecht and Hoopes, 2014, p. 14). The difference between a fraud audit and a financial audit is simple: one is designed to protect investors and provide the public with reasonable assurance that the financial statements are presented fairly and the other is specifically designed to catch fraud (Albrecht and Hoopes, 2014). The fraud audit is not an opportunity for auditors to provide an opinion, it is an investigation. While one would think that the fraud audit is a panacea, there are some downsides. The fraud audit, due to its extensive detailed nature, takes much more time to complete and as a result is considerably costlier than the financial audit. Despite the cons associated with the fraud audit, performing it is the only way to guarantee auditors will catch material financial statement fraud (Albrecht and Hoopes, 2014).

So why doesn't the accounting world use the fraud audit? While it could one day, the following line of reasoning makes it easy to understand why the accounting world hasn't made the fraud audit mandatory and why fraudulent activity is increasing. Companies are already spending money on the financial audit and the accounting world would most likely receive significant pushback from companies if it were to significantly increase the costs necessary to be in compliance. In a world that revolves around profit, decreasing the profit margin is generally not seen as a good thing. Furthermore, mandating the fraud audit could cause many smaller businesses to suffer, as they might not have the funds necessary to perform both audits. Additionally, fraudsters, specifically those at the management and executive levels, are able to thwart audits and avoid detection because they are in a position to steer the auditor in different directions (Singleton & Singleton, 2007). Seeing how management/executives would have a say in whether or not to perform a fraud audit as it is not required, a corrupt management is not going to agree to, let alone pay for the one tool specifically designed to catch them.

So where does that leave auditors? If the financial audit, and in turn auditors, are catching all material fraud, yet achieving such a small detection rate, how can the gap between frauds that occur and frauds that are detected be reduced? Obviously, if the fraud audit is not made mandatory, then the financial audit will continue to be the main detection method for fraud. As such, the accounting world needs to improve the ability of the financial audit to detect fraud at all levels. One way to do so is to improve the quality of the auditors performing the financial audit. It is my opinion that the starting point for such improvements should be auditors' training, and I am not alone.

Forensic Accounting

One option to improve the training of auditors is to include courses on forensic accounting. Forensic accounting is known as "the area that deals with the study of financial fraud and malfeasance" (Mitrić et al, 2012, p.65). Though there is no set definition, the one most commonly used is the one provided by the ACFE (Association of Certified Fraud Examiners) which defines forensic accounting as:

> a set of skills to use in potential or actual civil or criminal cases, including generally accepted accounting ones; determining loss of profits, revenue, or property or damage, assessment of internal controls, fraud and everything else that leads to the applying of accounting knowledge to the legal system (Mitrić et al, 2012, p. 65).

The lack of forensic accounting courses present in accounting curricula is cited by many as a reason that fraud has continued to exist, as students are not fully prepared to recognize fraud when they encounter it (Daniels et al, 2013). In an effort to increase the auditor's skills, several business schools have implemented forensic accounting courses hoping that it would enable students to better understand the elements of fraud. However, despite these improvements the majority of

business schools have been slow to adopt forensic accounting courses. In fact, studies have shown that not only has the adoption of forensic accounting courses been slow, but also the majority of business schools don't have specified courses designed to teach students about fraud or forensic accounting (Daniels et al, 2013).

Researchers in the accounting field are not the only ones who believe that accounting students would benefit greatly from forensic accounting classes. The National Commission on Fraudulent Financial Reporting (NCFFR) has stated that in accounting curricula:

> Educators should foster an understanding of the factors that may cause fraudulent financial reporting. In addition, it noted that rigorous and thorough academic preparation will assist students in gaining leadership employment and help them face the challenge of preventing and detecting fraud…teaching fraud and forensic accounting will enable students to acquire the necessary knowledge, skills, and abilities to combat fraud in today's accounting profession (NCFE 1978 & Daniels et al, 2013, p. 95).

I can say that during my time as a student at Texas Christian University (TCU), and I realize this is just one school out of thousands, my encounter with fraud, and fraud related topics, has been somewhat limited. There is the standard audit class where fraud is discussed, but there is no set class dedicated to understanding fraud and its various components. One would think that as one of the major issues auditors are expected to combat there would be more focus on fraudulent activity, including: how to recognize it, investigate it, respond to it, and circumvent management's potential manipulations. Currently at TCU there is a section for an accounting elective in the fall semester of senior year. A simple way to include a forensic accounting course into TCU's current program would be to make forensic accounting the required accounting elective. Additionally, the

accounting program allows for several free electives throughout the four-year time frame. An alternative solution to the one previously proposed would be to take away one of these free electives to make room for a required forensic accounting course. In truth, there are multiple avenues that can be pursued to implement such courses, making it a feasible option. In fact, several Universities across the country have already implemented courses specializing in forensic accounting (Carpenter et al, 2011). However, if only some schools are increasing accounting students' exposure to such a topic, then only some auditors are receiving better training. If the goal is to improve the financial audit's fraud detection rate, then all auditors need to receive better training, not just some. Now there are individuals that might argue accounting firms should provide such training for their employees rather than Universities. However, I believe that implementing forensic accounting training through courses that occur over a semester will give students the most time to understand and grasp the material. Additionally, it is in the standard audit class that students are introduced to the term professional skepticism, an important skill an auditor must possess to detect fraud. By offering an audit class, as well as a forensic accounting class, students/auditors can further improve their professional skepticism skills.

Professional skepticism is defined as "auditor judgments and decisions that reflect a heightened assessment of the risk that an assertion is incorrect, conditional on the information available to the auditor" (Nelson 2009 & Carpenter et al, 2011, p. 2). The use of professional skepticism by auditors is an incredibly valuable tool. Though professional skepticism is currently already taught in accounting curricula, adding a forensic accounting class will provide more in depth training for students, enabling them to detect more fraud. In Carpenter et al (2011) researchers followed two groups of students. One group was enrolled in a forensic accounting course in addition to the traditional audit course, and the other that was solely enrolled in the

traditional audit course. The researchers found that of the two groups, the students who had been trained in forensic accounting had a higher level of professional skepticism and were "more likely than untrained students to be open to the possibility of fraud when there are indications that fraud might be present" (Carpenter et al, 2011, pp 10-13).

Clearly forensic accounting courses can better prepare an auditor to understand the various elements of fraud and enhance their ability to use professional skepticism. Consequently, if the auditors performing the financial audit are better able to detect fraud, then their success can be extended to improve the financial audit's detection rate. However, it is not enough in my opinion to simply lecture students about the importance of professional skepticism, or tactics that can be used to detect fraud. To truly enhance the auditor's ability to utilize professional skepticism in an effective manner, thereby increasing the effectiveness of the financial audit, accounting students should be exposed to classes where they are trained in deception detection methods. These classes would expand professional skepticism even further to encompass human interactions, enabling auditors to avoid potential manipulation when engaged in an audit.

Deception Detection

Though technology can also be used to detect criminals through measures such as Big Data Analytics as discussed earlier, considering the human element when discussing fraud is a key component of detection. Especially when considering the ability of the perpetrator, specifically when at the management and executive levels, to steer the auditor away from the fraud and cover their tracks (Ramamoorti, 2008). To many, this simply means considering the psychology of the fraud perpetrator. However, I think it should be extended so that the auditor has training in understanding and reading human behavior to avoid manipulation.

One of the previously mentioned issues that occurs with the inclusion of technology in the workplace is verifying the authenticity of documents. Though in many cases the audit team is working on these types of documents, there are still interactions with management as the auditor goes through the audit planning process, as well as the process of acquiring documents. Instead of just considering these conversations as part of the audit process, auditors should be taught to treat each exchange with the client as an interview.

If auditors increase the depth of their professional skepticism to encompass interactions with the client, then they will improve their chances of detecting suspicious activity and potential frauds. Treating each interaction as an interview is just one small way to do so. Now I am not saying that auditors should interrogate their clients, but they should observe the client's behavior as they ask any questions related to the audit. By being able to identify behavioral patterns of deception when working with clients, auditors increase the tools available to them in terms of detecting fraud (Wells, 2001).

Identifying patterns of deception means taking note of both verbal and non-verbal cues. Verbal cues of dishonest individuals typically center on the following: repetition of the question, oaths, overuse of respect, avoidance of emotive words, and answering with a question. Just listening to the client and being aware of verbal warning signs would increase the ability of the auditor to use his/her professional skepticism. However, it is equally important to pay attention to nonverbal cues (Wells, 2001).

Non-verbal cues are incredibly hard to hide, as they are an integral part of our physiology. These movements are the body's way of soothing itself when placed under emotional stress, such as lying. Non-verbal cues of deception include, but are not limited to: assuming a fleeing position (pointing feet towards the door), constantly switching positions or fidgeting, the use of crossing

motions to make the body feel protected, or covering the mouth when speaking, and finally - if applicable - the individual's reaction to evidence (often times they will push the evidence away to avoid seeming interesting) (Wells, 2001).

Identifying these verbal and non-verbal cues of deception however, is actually a very complex matter. Researchers have found that the suspicion of deception is affected by the individual's demeanor. Demeanor alters the perception of whether or not a person appears to be telling the truth or lying, and is relatively independent of his/her actual level of deception. Some people just come off as more trustworthy than others and this makes it more difficult to determine whether or not someone is being deceitful (Van Swol et al., 2015: Levine et al., 2011). Researchers in Van Swol et al. (2011) have created two categories for demeanor: 1) honest (pleasant, composed, confident, and delivers plausible explanations) and 2) dishonest (where the individual exhibits some of the clues mentioned above). Aside from demeanor, another reason that individuals have a hard time detecting deception is that they have a bias to assume the individual is being honest unless there is an explicit reason to be suspicious of them (Van Swol et al., 2015; McCornack & Parks, 1986; Miller, Mongeau & Sleight, 1986; O'Sullivan, Ekman & Friesen, 1988; Zuckerman, et al., 1979; Zuckerman, DePaulo & Rosenthal, 1981).

Because there are several factors that could thwart and auditor's ability to identify deception in individuals, real life training should be implemented into accounting curricula in order to prepare them for their auditing duties. It is one thing to read about fraud on paper, however students should have the opportunity to participate in classes that put their knowledge of fraud and deception training to use through case studies and practice. Doing so will allow auditors to practice and hone their skills before they are out on the job. Though the audit does utilize technologies to help improve its effectiveness, the human element of fraud should not be overlooked.

Incorporating deception training into accounting curricula will increase the tools that auditors have at their disposal and consequently improve the ability of the financial audit to detect fraud.

Though the inclusion of such training may seem like a dreamlike solution that would not be feasible to implement, it is actually more possible than one might think. Currently, when people think of expert interrogators they think of government agencies such as the Secret Service, Federal Bureau of Investigation, or the Central Intelligence agency. What is not widely known is that the training these agencies go through to learn these interrogation skills, is actually available to the public.

Dr. Paul Ekman, a former Professor in Psychology at the University of California and a co-discover of micro expressions, is known for his extensive research on understanding and evaluating non-verbal behavior. Following his retirement from the University of California he created the Paul Ekman Group (PEG). PEG offers several online tools that allow users to learn how to evaluate these non-verbal cues. The two main online training tools are Micro Facial Expressions and Subtle Facial expressions. Both of these course have "proven to be useful not only to law enforcement and national security firms, but also to therapists, health professionals, salespeople, HR professionals, and negotiators" (paulekman.com). It is my recommendation that these online courses be incorporated into a class setting and paired with Ekman's published works, in order to give students, the training they need to detect various human elements of deception.

As with the inclusion of forensic accounting courses discussed earlier, these deception courses should not replace existing accounting curricula, but should complement it. Deception courses can be incorporated as an elective, or take the place of a free elective. If a University has constrained resources, the class could function in an online setting as Ekman's materials are already online. If the deception detection courses were offered to students online, I believe having

a lab component would enable students to practice in a real setting and enhance their detection skills even further.

IMPLICATIONS

Fraud is a growing epidemic that affects the global community, not just CPA's and certainly not just academics. The auditor's job is to detect material misstatement, including those related to fraud, and provide and opinion on financial statements in regards to their reasonableness. The financial statements are not only an integral part of the company, but many external stakeholders rely on them to make financial decisions. As a result, when auditors provide an opinion on the reasonableness of the financial statements they are providing peace of mind to stakeholders. Additionally, by detecting frauds auditors are detecting criminal acts, thereby bringing these criminals to justice.

Though auditors are currently detecting these material misstatements, there is a vast majority of frauds that are going undetected, and in turn criminals that are going unpunished. Additionally, with the increasing inclusion of computers and cloud based technologies into the workplace, criminals have greater opportunity to engage in fraudulent activity than ever before. The accounting world has already attempted to change legislation to combat fraud, however these changes have had little success. One possible change in legislation that could be extremely successful in detecting fraud, is mandating the fraud audit. However, at this point in time, such an enactment would receive significant pushback from the business community. There is another option available to the accounting world that would decrease the gap between the frauds that occur and the frauds that are detected, while maintaining the peace. Such an option is improving the training of auditors by including courses on forensic accounting and deception detection in accounting curricula.

Currently, auditors consider the human element and psychology of the criminal through the fraud triangle. However, technology has drastically impacted the fraud triangle making it easier than ever for a criminal to move through the three segments and come to the conclusion to commit the fraud. Though businesses use more technology than ever before, there is still a great deal of face to face communication that occurs during the audit process. By implementing the aforementioned courses, auditors will be able to expand their knowledge of fraud, allowing them to better identify and react to it, as well as expand their professional skepticism to encompass face to face interactions. Although forensic accounting and deception detection courses will not guarantee the auditor will catch all fraud, they will be able to cue in on areas they believe require investigation which could lead to more fraud detection. In short, fraud is a growing issue and if the financial audit is currently the main detection method, then improving its effectiveness can lead to a higher fraud detection rate. One simple way to improve the effectiveness of the financial audit, is to improve the effectiveness of those performing it, the auditors.

If this is done successfully, the results will be threefold. First, the financial audit's current detection rate of 10 percent will be increased, as more frauds will be detected. Second, as more frauds are detected, criminals will be prosecuted and the perception that fraud can be committed and concealed successfully will be greatly reduced. As such, criminals will not have the perception of opportunity for fraud they do now, which could lead to less frauds being committed. Finally, with these changes, the amount of money lost to fraud will be decreased enabling firms to use that money elsewhere. Such uses could include: an increase in payouts to shareholders, reinvesting the funds into the company, or investing in the community. Whatever avenue firms choose, the money will be where it belongs and not in the hands of a criminal.

CONCLUSION

Fraud is not a new topic. It is something the accounting world has continued to deal with year after year. Though auditors are meeting the requirements of providing opinions as to the reasonableness of financial statements, they are not adequately combatting fraud. The frauds auditors identify are material, leaving immaterial frauds to operate under the radar for years, as well as increasing the perception among criminals that a fraud can be committed and concealed successfully. The financial audit is not detecting all the frauds taking place because it is not designed to. Additionally, the inclusion of technology in the workplace has created a new avenue for fraud perpetrators to engage in fraudulent activity, making it easier than ever before. The accounting world must respond to these changes if it wants to effectively combat the growing fraud issue.

One of the major tools that the financial audit uses is the fraud triangle, which is used to understand the psychology of criminals and evaluate the risk of fraud by understanding the conditions under which fraud is likely to occur. The inclusion of technology has increased opportunity significantly making it easier than ever to commit and conceal a fraudulent act. Such an impact on opportunity has made rationalization easier than ever, because a criminal can justify the act simply by believing they won't get caught. Additionally, with the impacts to opportunity and rationalization, the incentives segment of the fraud triangle is less important than ever before. No one is going to turn down the opportunity for more money, and the sheer ease of committing the fraud can be incentive enough. As a result, frauds are being committed at an increasing rate and the financial audit, as well as financial auditors, just cannot keep up.

Although the financial audit has a relatively low fraud detection rate, the accounting world does have another tool at its disposal that is designed to catch fraud operating at all levels. The

fraud audit is specifically designed to catch fraud and dives further in depth in its investigation tactics to uncover deceptive behavior. However, while the fraud audit is extremely successful in detecting fraud, it is unlikely it will be used on a large scale. The fraud audit is currently not required for any company. Though companies can elect to partake in a fraud audit, a corrupt management is highly unlikely to partake in, let alone pay for, something that could convict them. Additionally, the added costs of the fraud audit are a major deterrent for corporations, especially smaller organizations.

However, the accounting world can improve the ability of the financial audit to detect fraudulent activity, not through legislation or rules, but rather through the people performing the audit. The auditors are on the front lines of the battle against fraud. By improving their effectiveness in detecting fraud, the effectiveness of the financial audit is improved as well. One way to do this is through the auditor's training, specifically by implementing changes in accounting curricula. By including courses on forensic accounting, the auditors' understanding of fraud is improved, enabling them to better identify and address it.

However, changes to accounting curricula should not end with the inclusion of forensic accounting courses. Rather, changes to accounting curricula should be taken one step further to include courses on deception detection. Though companies typically rely on electronic documents, there is still human interaction between the auditors and their clients. Since the fraud triangle has been impacted so significantly by technology, training auditors in deception detection will provide another avenue for them to evaluate the human element of fraud. Thus allowing auditors to evaluate interactions in real time rather than in a planning process. By including deception detection courses, auditors will be better equipped to recognize deception and thus can investigate any suspicious activity, which could increase the rate at which fraud is uncovered. Though it is a

small step, improving the training of auditors will increase their professional skepticism skills and greatly improve their ability to recognize signs of fraud and address it. As the auditors detection skills are improved, the ability of the financial audit to detect fraud will be improved as well.

APPENDIX A: THE FRAUD TRIANGLE

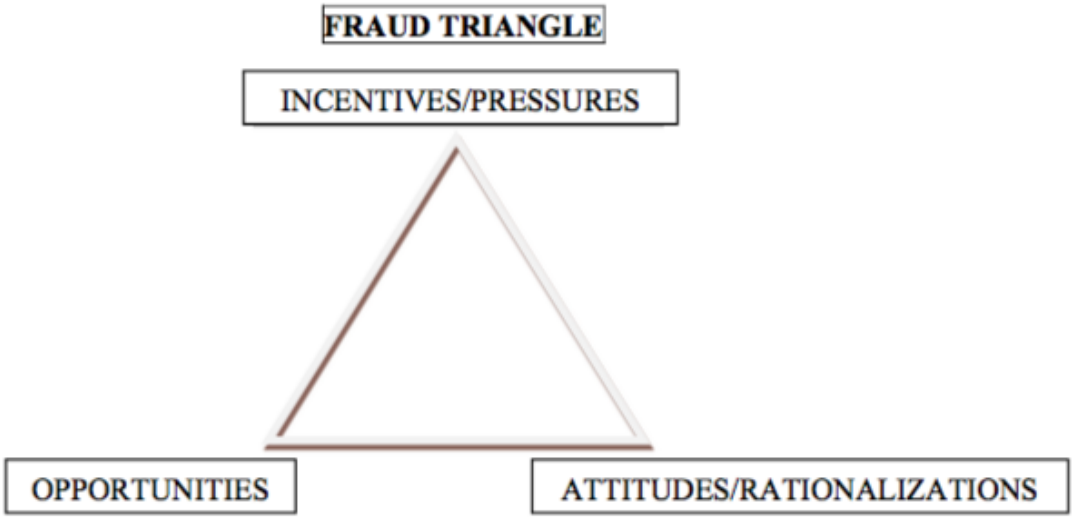

Figure Adapted from Buchholz (2012)

REFERENCES

Alali, F., A. & Yeh, C. (2012). Cloud Computing: Overview and Risk Analysis. *Journal of Information Systems,* 26(2), 13-33.

Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, and A. Konwinski. 2010. A view of cloud computing. *Communications of the ACM* 53 (4), 50-58.

Association of Certified Fraud Examiners (ACFE). 2008. *2008 Report to the Nation on Occupational Fraud and Abuse.* Austin, TX: ACFE.

ACFE Report to the Nation on Occupation Fraud & Abuse, Association of Certified Fraud Examiners (2012). 10-39.

Albrecht, S. and Hoopes, J. (2014). Why Audits Cannot Detect All Fraud. *CPA Journal.* 84(10), 12-21.

Buchholz, A. K. (2012). SAS 99: Deconstructing the fraud triangle and some classroom suggestions. *Journal of Leadership, Accountability and Ethics*, *9*(2), 109-118.

Collins, J. C. (2015). Technology Q&A. *Journal of Accountancy,* 220(3), 106-111.

Carpenter, T. D., Durtschi, C., & Gaynor, L. M. (2011). The Incremental Benefits of a Forensic Accounting Course on Skepticism and Fraud-Related Judgments. *Issues in Accounting Education,* 26(1), 1-21.

Cressey, D. R. 1973. *Other People's Money.* Montclair, NJ: Patterson Smith.

Daniels, B. W., Ellis, Y., Gupta, R.D. (2013). Accounting Educators and Practitioners' Perspectives on Fraud and Forensic Accounting Topics in the Accounting Curriculum. *Journal of Legal, Ethical & Regulatory Issues,*16(2), 93-106.

Festinger, L., & Carlsmith, J. M. (1959). Cognitive consequences of forced compliance. *Journal of Abnormal and Social Psychology*, *58*, 203-210. http://doi.org/cs4.

Generally Accepted Auditing Standards. *Standards of Field Work.* AU § 150.02.

Guillot, C. (2013). Opportunity for Fraud. *Internal Auditor,* 70(4), 43-46.

Hays, J.B. & Ariail, D. L. (2013). Enron Should Not Have Been a Surprise and the Next Major Fraud Should Not Be Either. *Journal of Accounting & Finance*, 13(3), 134-135.

Jaeger, J. (2014). Using Big Data to Find Fraud? First, Find the Data. *Compliance Week*, 11(122), 52-53.

Jamal, K. (2008). Mandatory Audit of Financial Reporting: A Failed Strategy for Dealing with Fraud. *Accounting Perspectives.* 7 (2), 97-110.

Jansen, W., and T. Granee. 2011. *Guidelines on Security and Privacy in Public Cloud Computing.* NIST Special Publication 800-144. Gaithersburg, MD: NIST.

KPMG. 2010. Audit in the cloud: Security audits versus cloud computing. Available at: http://www.slideshare.net/eburon/audit-in-the-cloud-kpmg

Kumar, R. 2002. Managing risks in IT projects: An options perspective. Information and Management (October): 63–74.

Levine, T. R., Serota, K. B., Shulman, H., Clare, D. D., Park, H. S., Shaw, A. S., & Lee J. H. (2011). Sender demeanor: Individual differences in sender believability have a powerful impact on deception detection judgments. *Human Communication Research*, *37*, 377-403. doi:10.1111/j.1468-2958.2011.01407.x

Lord, A. T. (2010). The Prevalence of Fraud: What Should We, As Academics, Be Doing to Address the Problem. *Accounting & Management Information Systems,* 9(1), 4-21.

McCornack, S. A., & Parks, M. R. (1986). Deception detection and relationship development: The other side of trust. In M. L. McLaughlin (Ed.), *Communication Yearbook 9* (pp. 377- 389). Beverly Hill, CA: Sage.

Miller, G. R., Mongeau, P. A., & Sleight, C. (1986). Fudging with friends and lying to lovers: Deceptive communication in personal relationships. *Journal of Social and Personal Relationships*, *3*, 495-512. doi:10.1177/0265407586034006

Mitrič, M., Stanković, A., Lakićević, A., (2012). Forensic Accounting – the Missing Link in Education and Practice. *Management (1820-0222),* (65), 41-50.

Newman, R. (2009). COMPUTER FORENSICS FRAUD INVESTIGATIONS. *Journal of Forensic Studies in Accounting & Business*, *1*(1), 69-81.

National Commission of Fraudulent Financial Reporting (NCFFR). 1987. Report of the national commission on fraudulent financial reporting. October 1987. Washington, D.C.: NCFFR.

Osmundson, J. S., J. B. Michael, and M. J. Machniak. 2003. Quality management metrics for software development. Information and Management 40 (8): 799–812.

O'Sullivan, M., Ekman, P., & Friesen, W. V. (1988). The effect of comparisons on detecting deceit. *Journal of Nonverbal Behavior*, *12*(3, Pt. 1), 203-215. doi:10.1007/BF00987488

Patterson, E. R. and Smith J. R., (2007). The Effects of Sarbanes-Oxley on Auditing and Internal Control Strength. *The Accounting Review*, 82 (2), 427-455.

Pearson, T. A., & Singleton, T. W. (2008). Fraud and forensic accounting in the digital environment. *Issues in Accounting Education*, 23(4), 545-559.

Singleton, A. J., Bologna, G. J., and R. J. Lindquist. (2006). *Fraud Auditing and Forensic Accounting.* 3rd edition. Hoboken, NJ: John Wiley and Sons, Inc.

Singleton, T. W., & Singleton, A. J. (2007). Why don't we detect more fraud? *Journal of Corporate Accounting & Finance*, *18*(4), 7-10.

Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education*, *23*(4), 521-533.

Van Swol, L., M., Braun, M. T., & Kolb, M., R. (2015). Deception, Detection, Demeanor, and Truth Bias in Face-to-Face and Computer-Mediated Communication. *Communication Research,* 42(8), 116-142.

Verschoor, C. C. (2015). Overcoming the fraud triangle. *Strategic Finance,* 97(7), 17-18.

Wallace, L., M. Keil, and A. Rai. 2004. Understanding software project risk: A cluster analysis. Information and Management 43: 115–125.

Wells, J., T. (2001). A Fish Story – Or Not? *Journal of Accountancy,* 192(5), 114-117.

Yu-Lun, L. & Ching-Jui, K. (2014). Cognitive Dissonance, Social Comparison, and Disseminating Untruthful or Negative Truthful eWOM Messages. *Social Behavior & Personality: An International Journal,* 42(6), 979-994.

Zuckerman, M., DeFrank, R. S., Hall, J. A., Larrance, D. T., & Rosenthal, R. (1979). Facial and vocal cues of deception and honesty. *Journal of Experimental Social Psychology*, *15*, 378- 396. doi:10.1016/0022-1031(79)90045-3

Zuckerman, M., DePaulo, B. M., & Rosenthal, R. (1981). Verbal and nonverbal communication of deception. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 14, pp. 1-59). New York, NY: Academic Press.