Straight from the Horse's mouth: Auditors' on Fraud Detection and Prevention, Roles of Technology, and White-Collars Getting Splattered with Red!

Aditya Simha
University of Wisconsin – Whitewater

Sandhya Satyanarayan
Independent Scholar

Fraud is increasingly an enormous problem for organizations all over the world today – the losses occurring due to fraud are over several billion dollars every year alone (Smith, 2008). In this article, we provide a thorough review of the extant literature on fraud, and conduct a qualitative interview (N=18) based study on forensic auditors' perceptions of fraud detection and fraud prevention methods, as well as their impression of the role of technology in fraud. We then highlight a rarely addressed problem – that of physical safety concerns that forensic auditors have to face while investigating fraud investigations. We finally suggest some directions for further research.

INTRODUCTION

Honesty for the most part is less profitable than dishonesty – Plato

The above mentioned quote by Plato has certainly been taken to heart by a lot of individuals, if one goes by the enormity and scale of fraud in organizational settings. Recent estimates have placed the loss occurring due to fraud as being as high as several billion dollars every year in developed countries alone - in Australia and the United Kingdom for instance; the cost of fraud is estimated as being about A$10 billion and £20 billion respectively (Smith, 2008). Similarly, Rossouw (2000) also mentions that fraud is a serious problem facing organizations in developing nations, and he asserts that the problem is further amplified as they face a serious and urgent need to engage in economic growth and development, and fraud prevents and hampers their growth and competitiveness. Fraud also tends to erode investor confidence in financial markets thereby compounding the problem (Peterson and Buckhoff, 2004; Rezaee et al., 2004).

The Association of Certified Fraud Examiners (ACFE) too estimated that annual fraud losses are approximately 5% of the annual revenues of organizations which translates to about $3.7 trillion (ACFE, 2014). This number has certainly risen in magnitude, if one just considers that the amount was $652 billion in 2006, which then shot up to $994 billion in 2008, and then to 2.9 trillion in 2010 (ACFE, 2006, 2008, 2010; Kaplan et al., 2010; Murphy and Dacin, 2011), and then to 3.5 trillion in 2012 (ACFE, 2012). A survey found that about one third of organizations operating worldwide are victims of fraud (PricewaterhouseCoopers, 2009). Similarly, fraud tends to adversely affect a very broad range of

stakeholders including audit committee and board members, top managers, employees, auditors, creditors, shareholders, and pensioners (Dyck et al., 2010; Kaplan et al., 2010).

This high rate of fraud and the resultant damage has certainly not escaped scrutiny or study by researchers – several studies have been devoted towards studying and examining fraud, in several settings (Alleyne and Howard, 2005; Archambeault, Webber, and Greenlee, 2014; Ashforth and Anand, 2003; Anand et al., 2004; Boolaky, 2012; Collins et al., 2009; Marcel and Cowen, 2014; Murphy and Dacin, 2011; Owusu-Ansah, Moyes, Oyelere, and Hay, 2002; Palmer, 2008; Rabl, 2011; Rabl and Kuhlmann, 2008; Sarens and Abdolmohammadi, 2011; Smith, 2008; Vanasco, 1998; Zahra, Priem, and Rasheed, 2005). Similarly, exposés of white-collar crime and situations of fraud are seemingly never-ending: the sordid details of grand schemes of fraud in organizations such as Enron, Credit Suisse First Boston, Global Crossing, Tyco, Waste Management, WorldCom, for instance have been widely documented (Brickey, 2006; Healy and Palepu, 2003; Ivancevich et al., 2003; Kulik et al., 2008; Rezaee, 2005; Sidak, 2003).

However, despite the presence of these different studies, there still is a lot of research and work that needs to and can be conducted on fraud, its prevention and detection, and other facets of fraud. Several calls for more research on how to understand fraud and prevent and detect it have been issued by different agencies and individuals (ACAP, 2008; AICPA, 2002; Carcello et al., 2009; Smith, 2008; Wells, 2004). Our paper is a response to those calls for more research.

In our survey of the literature on the topic of fraud, we happened to notice that there was a paucity of articles with rich qualitative data, especially articles that happened to utilize actual forensic auditors/investigators as participants in them. Our study aims to attempt to correct that imbalance. We conducted interviews with current forensic investigators who are actively investigating fraud situations in the field, as we felt that one of the best ways by which we could better understand fraud was by talking directly with the folks that dealt with it on a frequent basis. Another facet of our study sample is that these forensic investigators have had experience investigating fraud in several different countries, both developing and developed.

One of the chief purposes of this study was to add some depth and richness to the current reservoir of knowledge that exists on fraud. Our study aims to discover from currently active forensic investigators, their thoughts on fraud detection and prevention methods, as well as their thoughts on technology as it relates to fraud, and finally, their thoughts about the need for physical security in the work environment.

This paper is organized in the following way - our next section provides a detailed literature review of fraud in a forensic auditing and accounting context. Next we touch upon the different facets of fraud detection and fraud prevention methods, fraud and its relationship with technology, and then finally touch upon the physical security angle to forensic investigations. After doing so, we then introduce our study objectives, and then present our methodology section, followed by our results, and then finally present our discussion section. Our discussion section also provides suggestions for future research.

LITERATURE REVIEW OF FRAUD IN AN ACCOUNTING CONTEXT

Before embarking on a detailed literature synopsis on fraud, defining fraud may be beneficial. For the most part, *fraud* and *corruption* seem to have been used interchangeably in the literature base (for e.g., Ashforth and Anand, 2003; Anand et al., 2004; Collins et al., 2009; Marcel and Cowen, 2014); however, Rossouw (2000) tries and differentiates between the two concepts. He argues that this differentiation is essential because *corruption* tends to be mostly associated with the public sector and public officials, whereas *fraud* can occur in both the public as well as the private sector. Anyone in short, can be a perpetrator of fraud! Also, corruption inherently entails third-party involvement, whereas fraud can be a solitary act as well as a group act. The absence of third-party involvement in situations of fraud makes fraud much more difficult to detect, or to prevent even.

Rossouw (2000) defines *fraud* as "intentional deception by concealing or misrepresenting information that harms the financial interest of another person(s) and benefits the financial interests of the perpetrator" (p. 887). A more technical definition of fraud is provided by AICPA (2002, paragraph 5) and is as

follows, "fraud is an intentional act that results in a material misstatement in financial statements that are the subject of an audit." *Corruption* on the other hand is defined by Rabl (2011, p. 85) as "a deviant behavior that manifests itself in an abuse of a function in favor of another person or institution." In this paper, we chose to utilize Rossouw's and the AICPA's definitions of fraud, and therefore in our recruitment of study participants, we chose to interview forensic investigators who were dealing with cases of fraud in the private sector as opposed to investigators who were dealing with and investigating cases of governmental corruption.

One major reason that has been suggested as being the cause of fraud in many a case is the high pressure that corporate management has to face in order to achieve earnings targets. If those targets are missed, significant declines in the stock price ensue, and that in turn drives down and reduces executive compensation, as that is frequently tied in to stock price and earnings targets (Carpenter and Reimers, 2005). The Public Oversight Board (2000) too has identified this as being a frequent harbinger of fraud. Several empirical studies too have corroborated the finding that an excessive emphasis on earnings projections and aggressive management attitudes towards financial reporting were primary indicators of managerial motivation for fraudulent financial reporting (Albrecht and Romney, 1986; Bell and Carcello, 2000; Loebbecke et al., 1989).

This is very much linked to the fraud triangle (PCAOB, 2005), which suggests that three factors (opportunity, incentive/pressure, and attitude/rationalization) if all are present, predict the presence of fraud within an organization (Cohen et al., 2010; Murphy and Dacin, 2011). These elements in the triangle were first identified by Sutherland (1949) and then developed by Cressey (1953, p. 30, as cited in Cohen et al., 2010). Albrecht et al. (1982) started off the process of adapting the concept from criminology onto an accounting context, and identified 82 different fraud related variables, which they combined into three categories: situational pressures, opportunities to commit fraud and personal integrity (p. 37).

Auditing regulation through the ages has outlined numerous fraud-risk factors – the most recent standard, SAS No. 99 (AICPA, 2002, Para. 7), has organized risk factors by referring them to the three conditions generally present when fraud occurs. These definitions and risk-factors are directly aligned with and tied in to the fraud triangle (Cohen et al., 2010). A lot of empirical research has been carried out to demonstrate the importance of both the "incentives" and "opportunities" corners of the fraud triangle (for e.g., Albrecht and Romney, 1986; Loebbecke et al., 1989)

The first two corners of the fraud triangle have certainly been borne out as being associated with fraud (AICPA, 2002; Erickson et al., 2004; Graham et al., 2005; Murphy, 1999; Murphy and Dacin, 2011), however not as much attention seems to have been showered on the third corner (i.e. attitude/rationalization) of the fraud triangle (Carcello and Hermanson, 2008; Hogan et al., 2008; Murphy and Dacin, 2011; Wells, 2004), which led Murphy and Dacin (2011) to propose a framework that describes an individual's decision-making process when confronted with both opportunity and motivation to commit fraud. However, there still can be work attempted that would complement the current existing research on the third corner of the fraud triangle. As Cohen et al. (2010) attest, there is an increasing integration of the attitudes/rationalization factor into auditing regulation; however, despite that, there still needs to be a lot more research attempted to better understand the third corner.

Cohen et al. (2010) have also stressed that the third corner of the fraud triangle is also one of the most difficult one for auditors to assess, therefore it makes sense to try and see how and what auditors think about efforts to make it easier to assess this third corner of the fraud triangle. One of our aims in this study is to discover what forensic investigators think about criminal profiling and behavioral finance, as one way by which the third corner of the fraud triangle can be better understood is by bringing in concepts and strategies from criminal profiling and behavioral finance.

Rezaee (2005) found that five interactive factors explained several high-profile financial frauds – he categorized them into an interesting acronym (Cooks, Recipes, Incentives, Monitoring, and end results (CRIME)). Murphy and Dacin(2011) proposed a model wherein they described the psychological pathways to fraud for individuals, who believe that committing fraud is wrong. They propose three distinct pathways to fraud: (i) lack of awareness, (ii) intuition coupled with rationalization, and (iii)

reasoning. They also identify certain situational factors by which individuals commit fraud without even recognizing it. Their model is a useful one in proposing different interventions which can then be used to deter fraud.

We will now touch upon the different facets of fraud detection and fraud prevention methods, fraud and its relationship with technology, and then finally touch upon the physical security angle.

Fraud Detection Methods

Fraud detection involves identifying fraud as quickly as possible once it has been perpetrated (Bolton and Hand, 2002, p. 236), and these methods need to evolve in order to better detect fraud that perpetrators may have disguised better. Matsumura and Tucker (1992) were pivotal in developing an early theoretical foundation for fraud detection. Their empirical results supported a direct relationship between testing, fraud detection, and fraud prevention. Fraud detection methods have curiously enough not changed much for a very long time (Bishop, 2004) – this would perhaps explain why a lot of times fraud is "accidently discovered", although when one examines the difference between the percentages reported by the ACFE in 2004, and compares it to the percentage reported by the ACFE in 2014, one can notice that it's reduced a bit, and that today detection seems to rely more on tips from employees and other individuals (23.8% in 2004, and 40.2% in 2010). Johnson and Rudesill (2001) compile a list of guidelines that can be useful in fraud detection, and they also suggest that organizations need to make each and every employee responsible for detecting fraud incidences. Hassink et al. (2010) also examine the extent to which auditors comply with standards once fraud has been detected, and they found that auditors do not seem to comply with all standards properly.

One very interesting facet of fraud is that the median time span of reported frauds from their beginnings until detection is about 18 months, and there are quite a few frauds that last significantly longer than two years (ACFE, 2014; Lord, 2010), some types of frauds, such as check tampering and fraudulent financial statement fraud appear to go on for a much longer time and have a median time till discovery of about 27 months (ACFE, 2010).

It transpires that a lot of fraud cases are initially discovered by a tip or a complaint from an employee or from someone outside of the organization (ACFE, 2014). This pattern has been observed in prior ACFE studies as well (ACFE, 2012, 2010, 2008, 2006; Lord, 2010). One heartening conclusion can be reached though, which suggests that the Sarbanes-Oxley Act may be having a positive effect. It transpires that the percentage of frauds detected by internal controls reported by the most recent ACFE study (2014) appears to be higher than the percentage reported in the ACFE study in 2008 and previous years.

Some of the most commonly utilized fraud detection methods appear to be as follows – tips by insiders or outsiders, management review, by internal audit, by accident, by account reconciliation, document examination, external audit, surveillance/monitoring, notified by police, confession, and IT controls (ACFE, 2014, p. 19). This list is virtually identical to the one released by the ACFE in 2010, and suggests that fraud detection methods are mostly reactive measures and not proactive measures. Another compiled list of fraud detection methods was suggested by Bierstaker et al. (2006), however the methods on their compiled list fall into the ACFE categorization. Therefore, it makes sense to find out what active forensic investigators think about these fraud detection methods, and also see how they think these methods can be improved.

While some previous studies have looked into the question of the effectiveness of some of the fraud detection methods (e.g. Bierstaker et al., 2006; Blocher, 1992; Hylas and Ashton, 1982; Loebbecke et al., 1989; Wright and Ashton, 1989), they have mostly either been statistical analyses or survey based studies. While those studies are certainly important, and have added considerably to the existing literature base, there is definitely a need to supplement the knowledge base with some rich and interesting qualitative research on the topic. This is one of our purposes with this study, to be able to add some richness via our findings.

Fraud Prevention Methods

Fraud prevention on the other hand describes measures that are taken to stop fraud from occurring in the first place (Bolton and Hand, 2002, p. 235). Adams et al. (2006) argue that fraud prevention is the most cost-effective way to deal with financial loss through fraud, especially in light of the fact that companies that are defrauded are extremely unlikely to ever recover their losses. Bishop (2004) strongly advocates that preventing fraud needs to be made into a responsibility of each and every employee. Similarly, Ivancevich et al. (2003) delineate several responses that could be utilized to prevent and deter fraud in organizations.

Johnson and Rudesill (2001) assert that there are no sure-shot ways to completely eliminate fraud, but that with proper attention being bestowed on fraud prevention methods, organizations can hope to minimize the occurrences and losses. They provide a list of proactive tips that organizational managers can utilize in order to prevent occurrences of fraud from happening, many of which are similar to the list suggested by the ACFE (2010). Krummeck (2000) also asserted that fraud prevention methods need to be integrated completely with an ethics base, as not doing so, will render the process futile and useless.

The ACFE study in 2014 essentially found that anti-fraud controls or fraud prevention methods seemed to be quite effective; however it appears that smaller organizations are disproportionately victimized by occupational fraud than are their larger counterparts, although the variation between size categories is not much (ACFE, 2014). This disproportionate result may be in part due to the fact that smaller organizations have fewer anti-fraud control schemes in place.

Some of the most commonly utilized fraud prevention methods are as follows – surprise audits, job rotation/mandatory vacation, hotlines, employee support program, fraud training for employees as well as managers, internal audits, anti-fraud policy, external audit, code of conduct, management review, independent audit committee, management certification, and rewards to whistleblowers (ACFE, 2010, 2012). Here again, it makes sense to find out what active forensic investigators think about these fraud prevention methods, and also see how they think these methods can be improved. We again aim to add to the extant knowledge base on the topic with our study.

Fraud and Technology

The advent of technology and development has certainly brought in a lot of benefit to human society, however at the same time perpetrators have learnt to use technology in a negative way, and fraud has not been behind. Several financial fraudulent schemes have originated in a digital environment, and that typically involves using an IT-based solution to detect and handle cases of digital fraud (John, Jabber, and Sudarshan, 2012; Pearson and Singleton, 2008). This rise in sophisticated technology being (mis)utilized to perpetrate and commit fraud was predicted by Albanese (1988), where he predicts that fraud could become the crime of choice in the computer age. He also predicted that law enforcement would often lag behind the innovative techniques of criminals (p. 25).

The now presently ubiquitous presence of information systems in organizations has also contributed to the growth in technology related frauds. Schwartz and Wallin (2002) found that information systems tended to place a distance between the fraud and participants such that participants then chose to maximize their earnings. Essentially, information systems tend to depersonalize the situation, and make it easier for fraud to be committed. Similarly, Oates (2001) too suggested that technology makes it a lot easier for fraud to be committed via means of cyber crime incidences. Oates also cites the fact that technology tends to make it easier for individuals to maintain anonymity, which in turn makes them much more likely and liable to commit and engage in fraud (p. 93). The propensity of IT to be utilized in computer fraud is also elaborately described by Dippel (2000).

Some evidence does exist that suggests that while technology can be utilized negatively to commit crime and fraud, technology can also be utilized to combat crime and even detect and perhaps prevent fraud from happening (Fox, 2000; Flegel et al., 2010; Kakis, 1992; Pathria, 1999; Weatherford, 2002). Pearson and Singleton (2008) also point out that IT is being used to a great degree in fraud detection, and sometimes in fraud prevention. They mention that software such as data analytics and data-mining are

now being increasingly relied on during fraud detection processes. Some automated macros have also been developed by organizations to detect fraud (Albrecht et al., 2008; Pearson and Singleton, 2008).

However, in the end, technology and IT seem to having a rather "Dr. Jekyll and Mr. Hyde'ish" relationship with fraud. On the one hand, technology appears to be facilitating fraud, but then on the other hand it appears to be immensely useful in combating, detecting, and even preventing fraud from occurring. Therefore, asking forensic investigators their thoughts and opinions on this dichotomous relationship may be useful in better understanding the relationship between technology and fraud.

Fraud and Physical Security Risks

Most of the literature dealing with risks associated with fraud appears to be concerned with either the risks of fraud itself (Graham and Bedard, 2003; Knapp and Knapp, 2001; Wilks and Zimbleman, 2004; Zimbelman, 1997), or else appears to be concerned with the risks of auditors getting hit with lawsuits (Bonner et al., 1998; Kaplan, 1987; Lowe et al., 2002; Narayanan, 1994; Patterson and Wright, 2003). However, there have been some recent cases that suggest that not all risks are of a litigious nature, and that some risks pose serious harm to the auditors' physical well-being (Perri and Lichtenwald, 2007; Perri and Brody, 2011).

Perri and Lichtenwald (2007) proposed an addition to the FBI Criminal Classification Manual, and they suggested that a new homicide classification termed as *fraud-detection homicide* be included in the FBI's *Crime Classification Manual* (Douglas et al., 1992; Perri and Lichtenwald, 2007). In fact, Perri and Lichtenwald (2007) list about 27 known cases where homicide resulted as a result of fraud-detection, and the homicide was directed at the person(s) responsible for the fraud detection. They concluded that the homicides were not spur-of-the moment homicides, but that they were coldly calculated homicides (p. 29). Another study by Perri and Brody (2011) documented the case of Sallie Rohrbach who was an insurance auditor and was murdered during an investigation of fraud at an insurance agency. Both these studies seem to suggest that threats of physical violence are much more frequent than commonly thought. Perhaps, as is suggested by both studies, forensic auditors need to start becoming more cautious about their safety.

There does not seem to be much literature out there that delineates the safety risks that forensic auditors face – most research appears to be focused on litigious risks. However, there is reason to believe that forensic auditors (especially those in developing countries) have a valid reason to fear threats of physical reprisal. Since, there really isn't much literature on the topic, we believe that our study is one of the first few ones that examine the likelihood of physical reprisal against forensic investigators, and also take into account the perceptions of forensic auditors to determine the same. The next section outlines our study objectives.

STUDY OBJECTIVES

Our study attempts to add to the current knowledge base on fraud, fraud detection methods, fraud prevention methods, the relationship between fraud and technology, and physical safety issues that pertain to fraud investigators investigating fraud. As we mentioned earlier, qualitative studies will add richness to the extant literature base on fraud, and that is one of our primary purposes here with this qualitative research based study of ours. We also intend to shed some light on certain facets of fraud investigations that do not seem to have gotten as much attention as they ought to be getting.

We have chosen to undertake this study keeping four objectives in mind – (a) to discover forensic investigators' thoughts and perceptions on the effectiveness of current fraud detection and fraud prevention methods; (b) to discover forensic investigators' thoughts and perceptions on how to improve current fraud detection and fraud prevention methods; (c) to discover forensic investigators' thoughts and perceptions on the relationship between technology and fraud; and (d) to discover forensic investigators' thoughts and perceptions on the physical safety risks posed to them in the line of duty. Our specific research questions are as follows:

(i) What are forensic investigators' thoughts and perceptions on the effectiveness of current fraud detection and fraud prevention methods?
(ii) What are forensic investigators' thoughts and perceptions on how to improve current fraud detection and fraud prevention methods?
(iii) What are forensic investigators' thoughts and perceptions on the relationship between technology and fraud?
(iv) What are forensic investigators' thoughts and perceptions on the physical safety risks posed to them in the line of duty?

Our methodology section outlines the approach we took in order to achieve our four study objectives.

METHODOLOGY

Paradigm Guiding the Research

Our key interest in this study is to understand the phenomenon of fraud, fraud detection and prevention methods, the relationship between fraud and technology, and the physical safety risks associated with fraud investigations, from the perspective of forensic investigators. Since forensic investigators deal with fraud and the other mentioned facets of fraud on a very continual basis, we believe that our study's paradigm may be best classified as a phenomenological approach. Phenomenology is a perspective that advocates that knowledge can only be gained by understanding the direct, lived experience of others (McMillan and Wergin, 2006; Polkinghorne, 1989), and since we are essentially studying and trying to understand from the experiences of forensic investigators, we believe that the paradigm most appropriate for our research is that of phenomenology.

Research Design

Our study used a qualitative interview based method. Our interview based method was an in-depth, phenomenological based interview method (Kvale and Brinkman, 2009; Seidman, 2006). We used open-ended questions in our interviews, and also built upon and explored our participants' responses to pursue further exploration of their answers (Seidman, 2006). We followed Myers' (2009) advice about utilizing a semi-structured interview format as that would allow us to capture and obtain rich data. In addition to following a semi-structured interview format, we also followed the technique of mirroring which Myers and Newman (2007) suggest is a technique to ensure that our participants' language and perceptual vision of the world would be reflected in our analysis. We followed mirroring by using the words and phrases that our participants used to construct our comments to them through the interview process. We also ensured that we demonstrated triangulation of participants (Rubin and Rubin, 2005; Myers, 2009) by seeking out participants who were from different organizations and had different sorts of professional backgrounds and experiences.

Researcher as Instrument

Reflexivity is a very important mark of rigor in qualitative research, as it follows that researchers are pretty much the primary instrument in a qualitative study. Researchers shape not just the data but also affect the research process. The acknowledgment of prior assumptions and experiences, as well as personal and intellectual biases, is a very important way by which to address issues of validity and the trustworthiness of a study (Marshall and Rossman, 1999). We now provide a small discussion on how our assumptions and experiences support increased understanding of the forensic auditor perspective that is studied.

Both researchers involved in this study have had experience studying and researching fraud. One of the researchers has had over 10 years of experience in the field investigating fraud cases for organizations, and is also an active forensic auditor. The other researcher has had some experience studying and designing fraud detection software.

This experience on our parts has had a positive effect on our research, because when we study the perceptions and attitudes of our forensic auditor participants, we can certainly identify with them better and that helps us avoid errors of misunderstanding that can sometimes happen while analyzing the transcribed notes. At the same time though, since neither of us was directly involved in any of the cases or situations that our participants talked about, we were able to retain our independent objectivity while studying our participants.

During the duration of this study we took extensive field notes and also kept track of analytical insights through memos that were included in the data to be analyzed. We then engaged in researcher triangulation, which involved each researcher working individually with the raw data to perform open coding. We then came together as a team and engaged in a co-analysis and shaping of the final themes resultant from our data.

Participants, Recruitment, and Selection Procedures

The participants in this study were currently active forensic auditors, working at different organizations (including the big 4 accounting firms). A total of 18 auditors participated in the study. These auditors were predominantly from India; however they also had experience working in several countries besides India, including the United States, United Kingdom and South Africa. Their average experience in the field of forensic accounting and fraud investigation was about 16.7 years. 12 of our participants were male and the remaining 6 were female. Our participants had a varied range of professional backgrounds ranging from engineering backgrounds to police backgrounds to military backgrounds among others, however at present all our participants were actively working in the capacity of forensic auditors for accounting firms.

The sample size in qualitative research is typically determined by the researcher's estimation of the richness of data that participants generate, and the sample size also depends on the specific method that is used (Patton, 1990). Conventional knowledge posits that the number of required participants becomes obvious as studies progress, when new categories, themes or explanations stop emerging from the data, and data saturation occurs (Marshall, 1996; Seidman, 2009). In our case, we obtained data saturation at about 11 participants; however since we had already obtained consent from and fixed interview slots with the remaining participants, we continued to collect more data and finally obtained a total of 18 participants.

After obtaining approval from the university Institutional Review Board (IRB), we set about recruiting participants for the study. We obtained a list of potential candidates to interview from three senior partners that one of the researchers knew, and set about emailing those potential candidates. We emailed 21 different forensic auditors, and obtained 18 suitable participants from the lot. 2 auditors did not respond to our emails, and 1 refused to participate in the study. However, the remaining 18 agreed and were consequently interviewed by both of us. Our selection criterion was that our participants needed to have experience in forensic auditing and investigating fraud, and also needed to be currently active in the field.

Sources of Data

Data was collected through our in-depth interviews, which were obtained through telephonic interviews. The interviews were audio recorded and we took process notes during the interviews. The interviews were semi-structured interviews; and the interview protocol consisted of five questions. Each researcher also kept analytical memos and field notes which were included in the data to be analyzed.

Data Analysis and Management

The final data for analysis consisted of audio recordings and transcripts of the interviews, as well as the field notes and analytical memos. Two graduate students initially transcribed all the audio recordings, after which both the researchers then independently reviewed the text and recordings, and checked for omissions and errors. The field notes of both researchers were also used to address inconsistencies in the transcripts. The analysis of this qualitative data was handled by utilizing the method that Marshall and

Rossman (1999) and Myers (2009) suggest. The first step in the analysis of qualitative data requires that researchers immerse themselves in the data, and therefore, both the researchers independently read all transcripts and process notes and then performed open coding (Marshall and Rossman, 1999). The next step in the process of interpretation involved identifying the essence of the data. After both of us had completed this process of finding meaningful units in the data, we got together and discussed emerging themes in the data. At this point the analytical memos were also considered, and structural synthesis occurred (Marshall and Rossman, 1999).

RESULTS

The following five themes emerged from our data. In response to our first two research questions we obtained the following two themes – (i) Fraud Detection methods are inadequate and need to be urgently improved, and (ii) Fraud Prevention methods need to be made much more pronounced and ubiquitous. In response to our third research question we obtained the following theme – (iii) The dual role of technology in fraud, and in response to our fourth research question we obtained the following theme – (iv) Physical safety concerns are a valid threat, and need to be addressed by organizations. We also obtained an additional theme from our data, which was – (v) Training forensic auditors in behavioral finance and criminal profiling may be advantageous in detecting fraud and preventing physical safety concerns.

Inadequacy of Current Fraud Detection Methods and a Need for Their Improvement

Our participants were asked to tell us their perceptions of fraud detection methods. Almost all of our participants seemed to suggest that current fraud detection methods were not perfect and indeed in the words of one of our participants, "…. the problem is that [these] fraud detection methods are very reactive…. We only find the tip of the iceberg when using one of these detection methods… very inefficient methods…." (P11). Included below are some of the numerous statements made by our participants in this regard:

> "……most companies have these old detection methods that are not sufficient or adequate. Because of lack of active monitoring from station's perspective… so there's always a window of opportunity there for the perpetrator…." (P1)

> "…… a lot of fraud detection methods are much too old fashioned…. they include basic fundamentals such as document analysis and background checks, but they are not having any in-house facilities to detect fraud……. Understanding the network and network flow is still lacking a lot…. in my own experience we have had to start from scratch and learn the process and then start the investigation which is not helpful in handling a rigorous investigation" (P4)

> "….. but my feeling is that there are no real up-to-date methods of detecting fraud… in a few instances, I have seen some in the current environment….but still I think most of the fraud detection methods are based on reacting to the fraud and a bit too late….." (P5)

> "…. you know, the problem with fraud detection methods are that they are just too late…by the time, one gets to discover or detect the fraud, it's already too late….fraud detection methods will always have a lag time….. as long as the lag time is small, it should be fine, but that's not the case….right now, the lag times are increasingly long…." (P12)

We also obtained consensus among our participants that current fraud detection methods needed to be improved, and that the improvement needed to be effected on an important scale if fraud is to be detected

early enough. Included below are some of the numerous statements made by our participants in this regard:

> "….handwriting analysis is something that can be extremely useful…..especially in rural areas where there isn't much influence of computers…. If fraud detection methods could somehow incorporate handwriting analysis, it may be very useful…." (P4)

> "…. companies just don't have enough in-house capabilities to detect fraud…and they are not able to proactively monitor pressing issues and see if, "can there be fraud"… becoming proactive and changing the mindset of top-management is a must if companies need to improve their fraud detection methods…" (P7)

> "…. what we need is a method that has an element of surprise built into it….also, now detecting fraud is not happening because we wait for signs that randomly happen….. Rather than having to put certain things off, we need to have potential audits for everything to be able to better detect fraud…" (P8)

> "….some of the current methods in the US might not be here in India, because in the US it is more technology driven, India is more dividends driven….. we need to integrate and incorporate the latest software into fraud detection methods in India…." (P9)

> "….most fraud detection methods are like cancer detection kits, by the time you get to know that there is cancer (or) fraud in a person or organization, it's too late already… fraud detection methods must be added to and with fraud prevention methods…make it an integrated system, where both prevention and detection are handled together…if we make it impossible for people to commit fraud, it will be so much easier to catch them when they commit fraud…" (P14)

> "…a much more cohesive and formalized thought process needs to go in for improving fraud detection methods…. The lack of rigor of methodology is a prime reason for this…." (P18)

For the most part, all our participants seemed to suggest that in their opinion fraud detection methods were much too reactive, and therefore susceptible to serious time lags. After all, if fraud detection methods could somehow be improved such that a reduction could be brought about in the amount of time taken to detect fraud, the severity of fraud would be reduced significantly. Similarly, several of our participants also suggested that fraud detection methods could be improved if the latest technology and software were to be incorporated into their design.

Augmentation in the Scale and Role of Fraud Prevention Methods Essential

Our participants were asked to tell us their perceptions of current fraud prevention methods. Most of our participants seemed to think that current methods of fraud prevention were fairly effective; however they did seem to suggest that these methods of fraud prevention and control needed to be augmented and utilized in a more amplified and increased fashion. The general consensus seemed to be that fraud prevention methods were not being used to the extent that they should be. Some examples that are indicative of this trend are as follows:

> "… fraud prevention and control is really important….where you highlight things on real time basis are those that can prevent the environment for fraud… more mechanisms are out there that can be used to prevent fraud…but they need to be implemented more…" (P3)

> "… There needs to be a better system for communication by which employees can report to their superiors or others if something fishy is going on…they should be able to report it to some third party. Also companies need to be able to track activity, and their controls need to incorporate that... right now, not all companies have that sort of system built in…." (P6)

> "…. one aspect of fraud control is that it needs to be both overt as well as hidden… overt control mechanisms will avoid most simple cases of fraud, while the hidden mechanisms will help prevent complicated fraud…. if all companies could get some sort of increased role of prevention methods in their functioning, fraud could be wiped out…" (P12)

> "…. fraud control is a really fine way to prevent fraud from occurring…. if people and employees know that there are mechanisms in place to monitor them if they screw up, they won't screw up… I just wish that more organizations would implement fraud control in the first place and not rely on detection…." (P16)

Part of the process of qualitative analysis also involves looking for disconfirming evidence. Most participants in the study had a positive opinion of fraud prevention and control methods and also felt that it was a proactive method as opposed to fraud detection methods. However, one participant seemed to disagree with the rest of the participants about the nature of fraud prevention methods. That participant seemed to suggest that prevention methods were also reactionary; however there was consensus with the other participants in that augmentation of fraud prevention methods

> "….both methods are very reactionary methods. It is often a reactionary measure to any kind of fraud, especially in India…. Also most companies do not have in house capabilities to solve problems, so they have to rely on other external agencies to assist them in investigations…. Maybe instead of reactive measures we should take a more proactive method of prevention or stopping the fraud…. the top management mindset has to change, they have to promote fraud prevention methods enthusiastically…." (P7)

The Dual Role of Technology in Fraud

We asked our participants to tell us their perceptions of the role that technology plays when it comes to fraud related situations. We found that on the whole, the general consensus from all our participants was that technology played a very dual role when it came to fraud. On the one hand, technology made it very possible and easy for perpetrators to commit fraud, but on the other hand, it also assisted auditors and investigators in their efforts to detect and prevent fraud. All our participants though seemed to recognize the potential benefits of harnessing technology to combat fraud. Some statements from them are provided below to better emphasize this theme:

> "… technology is definitely being used to commit fraud…Similarly, I think if you look at an anomaly I think most organizations monitor transactions, do analysis on transactions, but they don't do analysis on computer activity….companies definitely need to monitor computer activity of their employees more rigorously.." (P4)

> "…technology has its own set of pros and cons, we have to be aware of the situation and we also need to be more tech-savvy….I feel a forensic accountant needs to be a tech savvy person; he has to be a person who combines forensics with technology." (P6)

> "…now fraud you already know what happens, it is a technology loophole and those loopholes are used to hide accounts…for example, if there is some money lying in the pool, you can move it elsewhere and then bring it back to balance the sheet later on…

these kinds of things can be exploited using technology…there definitely needs to be supervision for technology…." (P7)

"….I would not want to consider technology a friend, nor as an enemy. It is just a tool at the end of the day. It depends, like an atom bomb or nuclear energy, it depends on the user. If you want to use it for good, you can, or if you want to use it destructively, you can. But I realize that as the day goes by a lot of investigators use technology. So it is important for the fraud investigators to be equally equipped with the latest technology… but it is one of the most difficult factors for investigators to keep themselves updated on the latest technology…" (P9)

"…. So, on one hand technology helps us to gather data, which is deleted over a period of time; on the other hand, technology is now helping subjects delete that data permanently. So that is one aspect, but I still feel that technology helps me in catching fraud…" (P11)

"…..technology can be a resource for you to counter fraud….but also, if you are not going to rely on anything but technology you are going to fail…" (P17)

One of our participants made a particularly emphatic point, which seems to tally very well with what most of the participants seemed to feel. That point is exemplified with the following statement:

"…. I definitely would prefer technology, with anything there is good and bad. With technology there are too many good things. I'd definitely go for technology, but we have to make sure that the technology we are implementing, we understand properly…" (P1)

Physical Safety Concerns are a Valid Threat and Need to be Addressed

Our participants were asked by us to relate whether they ever felt as if their physical safety and well-being was an issue during a forensic investigation, and whether they felt the need for physical security during an investigation. Most of our participants seemed to suggest that physical safety concerns were a very serious issue, and needed to be addressed by organizations. They especially felt that the need for physical safety was heightened when investigating fraud in remote locations. Some of their narratives are provided below to better contextualize this theme:

"….when I am in big cities I never felt any need for security but when I go to remote places, small towns, I am a bit concerned about my security… in one small town, the people we were investigating arranged a strike so they gathered outside the office and we had to leave right away…." (P1)

"….when the contract was allotted, it turned out that the beneficiary was a brother of a politically strong person… our client wants us to go and analyze the data at the physical location of that other place, even though it was located in a very unsafe location… it was infested with naxalite elements…." (P2)

"…. my team has had to say no twice to a client…the reason being that the client wanted us to investigate matters which when we did some digging into, we found that it was tied in with the underworld….we had to refuse and tell the client that they needed to contact the governmental authorities to do that job…" (P5)

"….what happens is when we start investigations there are sensitive times and there can be threats to your life that way….so sensitive crime is a hard bargain because you also

need to be worried about your family and your personal security is also very important…" (P7)

"…I have experienced this once….I was required to conduct certain interviews and during the interviews, they [interviewees] perceived it as a threat. It was in a remote area in [place deleted for confidentiality] and people were making enquiries about where we were staying and what we were detecting and things like that…." (P9)

"…a colleague of mine once continuously received threatening calls, at all times of the day and night….the police also was unable to do anything because the callers kept changing their SMS cards to avoid detection….but they felt that the calls were tied in with the investigation at the time, as the party concerned was a very powerful and influential person…" (P13)

Many participants also seemed to indicate that organizations needed to do something to ensure the safety of their forensic investigators. Some narratives to that effect are provided below:

"… I think organizations need to ensure that their forensic teams are provided with proper security arrangements… it may cost them a little bit more, but that amount is negligible in the long term…" (P12)

"… especially in some regions of the world, one has to be very careful about physical safety concerns…. I remember when I was sent to [name of place deleted], there was no real law structure in place there… my company sent us there, but they thoughtfully provided us with security personnel to accompany us there… I think more organizations need to do that…it's almost like they do not anticipate anything happening to threaten the auditors…." (P15)

Training in Behavioral Finance, Criminal Profiling, and Technology May be Beneficial in Combating Fraud

Another interesting theme emerged from our data – we had asked our participants to tell us about what kind of training methodologies would be most beneficial in training forensic auditors to combat fraud. We found that most of our participants seemed to think that criminal profiling and behavioral finance training would greatly benefit forensic investigators. We also found that our participants seemed to think that training in the latest technology and software would also help improve auditors' abilities to combat fraud. Some of the narratives around that theme follow:

"…. it can be helpful…sometimes we have a hunch that something is wrong, so having training in criminal profiling may help pick up on the behavior of the employee…to find that something is wrong….." (P1)

"…based on my initial experience as a police officer, I can definitely state that criminal profiling training will help…I will give you one example: one senior vice-president of a company had become a contact, he wanted us to investigate a case wherein he accused a few other top management guys of stealing money….we started investigating, this senior VP kept calling us and asking us for updates… and you know then we said this is not the right behavior of an innocent person…we found something very funny about this man…. Then during the final interview, I established an interface with the suspect and then we realized that the suspect was a witness…. And the VP was the actual guilty party… in an ironic way; he hired us to bust himself…" (P2)

> "… it would be a great advantage…. If a guy has already done criminal profiling properly it will help in investigations…when I was in the Army, we did criminal profiling on people especially the high level criminals for being involved in terrorist factories….. I think that organizations need to latch onto existing organizations to facilitate this sort of training…." (P6)

> "… training in criminal profiling and behavioral finance both help with fraud investigation teams….. with specific investigations, where you need to go beyond the documents, the things you can't see with your eyes, you need to understand the person you are investigating, their psyche and personality.." (P9)

> "… I feel they should because there are lots of instances when the behavior assessment is required. For example, when an open interview is undertaken it is more meaningful as the body language, the answers, expressions all convey a meaning and also help is modifying the interviewing approach to get the maximum information…." (P10)

> "… if auditors end up getting trained in diverse fields such as behavioral finance and criminal profiling, it will only add to their arsenal…I am confident that it will increase the success rate of forensic auditors'…." (P13)

However, as we mentioned earlier, searching for disconfirming evidence is part of the qualitative research process. One of our participants had a more cautious attitude towards training auditors in criminal profiling:

> "…. Yes and no for criminal profiling….we have to be careful about that training not coloring one's judgment…also, auditors need to make sure that they avoid stereotypes that may be generated due to criminal profiling….but then, criminal profiling training can facilitate out-of-the-box thinking, which is a positive aspect…" (P18).

DISCUSSION

Our study intended to better understand the phenomenon of fraud, and also glean from forensic investigators their thoughts and perceptions on four different matters – fraud detection and fraud prevention methods, the link between technology and fraud, and the physical safety issues arising from fraud investigation. We were interested in adding some rich depth to the work already conducted on fraud, as it appeared that rich qualitative data was not abundant in previous research on fraud.

Some limitations of our study are typical qualitative research issues – it is rather hard to generalize our findings to the entire population of forensic auditors in the world. However, we tried to make our findings as generalizable as we could by choosing several participants who had work experience in a few different countries (besides India). Also, while our qualitative data provided rich information about the auditors' perceptions on the different matters pertaining to fraud investigations, our sample was small. However, as we mentioned earlier, in qualitative research the sample size depends on when saturation of data occurs (Marshall, 1996; Seidman, 2009), and since we obtained data saturation at about 11 participants, our final sample of 18 is more than adequate.

Our findings indicate that forensic auditors seem to think that current fraud detection methods are not infallible, and indeed are quite prone to serious time lags. There is also the perception that these methods are too reactive, and need to somehow be improved such that the time lag between when the fraud is committed and when it is detected reduces. Similarly, our forensic auditors also seem to think that while current methods of fraud prevention are fairly effective, they need to be utilized more, and more organizations need to start utilizing them. This finding corroborates the findings of Bierstaker et al. (2006) when they found that small organizations in particular were not utilizing fraud prevention and

fraud control mechanisms, possibly due to the setting-up cost of doing so, even though fraud affects small organizations tremendously (ACFE, 2006, 2008, 2010).

Another finding of ours is with regard to the link between technology and fraud. Many of our participants identified technology as being a way for savvy fraudsters to commit fraud, and also identified technology loops as being very exploitable. However, they also recognized the positive role that technology plays in their being able to better detect and combat fraud. This suggests that the role of technology in fraud is a rather dichotomous one, but that on the whole, technology offers a lot more positive benefits and outcomes than negative ones.

Our findings have helped us understand the necessity for highlighting the physical safety risks that forensic auditors can very possibly face during the course of an investigation. While, one could argue perhaps that this may be a phenomenon unique to a developing country context, the number of cases in the US (Perri and Lichtenwald, 2007; Perri and Brodi, 2011) is testimony to the fact that this phenomenon is perhaps a lot more pervasive. Further research in this direction would be a welcome step as emphasizing and recognizing the possible dangers of fraud investigation is something that would benefit forensic investigators as well as their organizations.

We also found that our participants think that training auditors in behavioral finance and criminal profiling and the latest software will only help in the efforts to combat fraud. While, this kind of training may not be possible in-house, it is certainly feasible for organizations to tie up with other organizations and thereby reap the awards of increased success against fraud. Further research needs to be conducted on how exactly this sort of new training can be imparted to forensic auditors, such that it positively impacts their success rate in combating fraud.

On a final note, we must add that further research on fraud is an absolute necessity, especially in regard to improving fraud detection methods and implementing fraud prevention methods, and also in regard to ensuring that forensic auditors are shielded from potential harm during forensic investigations. After all, since fraud is typically considered a white-collared crime, it would only be judicious to keep the collars white, and not taint them with specks of red!

REFERENCES

Adams, G. W., Campbell D.R., Campbell, M. and Rose, M.P. (2006), "Fraud Prevention: An investment no one can afford to forego", *The CPA Journal.*

Advisory Committee on the Auditing Profession (ACAP) (2008), *Final Report of the Advisory Committee on the Auditing Profession,* United States Department of the Treasury, Washington, DC.

American Institute of Certified Public Accountants (AICPA) (2002, October), *SAS No. 99: Considerations of Fraud in a Financial Statement Audit,* AICPA, New York, NY.

Albanese, J. S. (1988), "Tomorrow's thieves", *The Futurist,* Vol. *22* No. 5**,** pp. 24-28.

Albrecht, W.S. and Romney, M.B. (1986), "Red-flagging management fraud: A validation", *Advances in Accounting,* Vol. 3**,** pp. 323-333.

Albrecht, S.W., Albrecht, C. and Albrecht, C.C. (2008), "Current trends in fraud and its detection", *Information Security Journal: A Global Perspective,* Vol. 17 No. 1, pp. 2-12.

Albrecht, W.S., Romney, M.B., Cherrington, D.J., Payne, I.R. and Roe, A.J. (1982), *How to Detect and Prevent Business Fraud,* Prentice-Hall, Englewood Cliffs, NJ.

Alleyne, P., and Howard, M. (2005), "An exploratory study of auditors' responsibility for fraud detection in Barbados", *Managerial Auditing Journal,* Vol. 20 No3, pp. 285-303.

Anand, V., Ashforth, B.E. and Joshi, M. (2004), "Business as usual: The acceptance and perpetuation of corruption in organizations", *Academy of Management Executive,* Vol. 18 No. 2, pp. 39-53.

Archambeault, D. S., Webber, S., & Greenlee, J. (2014), "Fraud and Corruption in US Nonprofit Entities A Summary of Press Reports 2008-2011", *Nonprofit and Voluntary Sector Quarterly*, 0899764014555987.

Ashforth, B.E. and Anand, V. (2003), "The normalization of corruption in organizations", *Research in Organizational Behavior,* Vol. 25, pp. 1-52.

Association of Certified Fraud Examiners (ACFE) (2004, October), *Report to the Nation on Occupational Fraud and Abuse* (ACFE, Austin, TX)
Association of Certified Fraud Examiners (ACFE) (2006, October), *Report to the Nation on Occupational Fraud and Abuse,* ACFE, Austin, TX.
Association of Certified Fraud Examiners (ACFE) (2008, October), *Report to the Nation on Occupational Fraud and Abuse,* ACFE, Austin, TX.
Association of Certified Fraud Examiners (ACFE) (2010, October), *Report to the Nation on Occupational Fraud and Abuse,* ACFE, Austin, TX.
Association of Certified Fraud Examiners (ACFE) (2012, October), *Report to the Nation on Occupational Fraud and Abuse,* ACFE, Austin, TX.
Association of Certified Fraud Examiners (ACFE) (2014, October), *Report to the Nation on Occupational Fraud and Abuse,* ACFE, Austin, TX.
Bell, T.B. and Carcello, J.V. (2000), "A decision aid for assessing the likelihood of fraudulent financial reporting", *Auditing: A Journal of Practice and Theory,* Vol. 19, pp. 169-184.
Bierstaker, J. L., Brody, R.G. and Pacini, C. (2006), "Accountants' perceptions regarding fraud detection and prevention methods", *Managerial Auditing Journal,* Vol. 21 No. 5, pp. 520-535.
Bishop, T.J.F. (2004), "Preventing, deterring, and detecting fraud: What works and what doesn't", *Journal of Investment Compliance,* Vol. 5 No. 2, pp. 120-127.
Blocher, E. (1992), *The Role of Analytical Procedures in Detecting Management Fraud,* Institute of Management Accountants, Montvale, NJ.
Bolton, R.J. and Hand, D.J. (2002), "Statistical fraud detection: A review", *Statistical Science,* Vol. 17 No. 3, pp. 235-255.
Boolaky, P. K. (2012), "Accounting development and international financial reporting standards in small island economies: The case of Mauritius between 1960 and 2008", *Journal of Accounting in Emerging Economies*, Vol. 2 No.1, pp. 4-29.
Bonner, S.E., Palmrose, Z-V. and Young, S.M. (1998), "Fraud type and auditor litigation: An analysis of SEC accounting and auditing enforcement releases", *The Accounting Review,* Vol. 73 No. 4, pp. 503-532.
Brickey, K.F. (2006), "In Enron's wake: Corporate executives on trial", *The Journal of Criminal Law and Criminology,* Vol. 96 No. 2, 397-433.
Carcello, J.V., Bedard, J.C. and Hermanson, D.R. (2009), "Responses of the American accounting association's tracking team to the recommendations of the advisor committee on the auditing profession", *Accounting Horizons,* Vol. 23 No. 1, pp. 69-84.
Carpenter, T.D., and Reimers, J.L. (2005), "Ethics and fraud in financial reporting", *Journal of Business Ethics,* Vol. 60, pp. 115-129.
Cohen, J., Ding, Y., Lesage, C. and Stolowy, H. (2010), "Corporate fraud and managers' behavior: Evidence from the press", *Journal of Business Ethics,* Vol. 92, pp. 271-315.
Collins, J.D., Uhlenbruck, K. and Rodriguez, P. (2009), "Why firms engage in corruption: A top management perspective", *Journal of Business Ethics,* Vol. 87 No. 1, pp. 89-108.
Cressey, D.R. (1953), *Other People's Money: A Study in the Social Psychology of Embezzlement,* The Free Press, Glencoe, Il.
Dippel, T. (2000), "IT as an enabler of computer Fraud", *Information Security Technical Report,* Vol. 5 No. 2, pp. 60-70.
Dyck, I.J.A., Morse A. and Zingales, L. (2010), "Who blows the whistle on corporate fraud", *Journal of Finance,* Vol. 65 No. 6, pp. 2213-2254.
Erickson, M., Hanlow, M. and Maydew, E.L. (2004), "How much will firms pay for earnings that do not exist? Evidence of taxes paid on allegedly fraudulent earnings", *The Accounting Review* Vol. 79 No. 2, pp. 397-408.
Fox, B.R. (2000), "Technology: The new weapon in the war on insurance fraud", *Defense Counsel Journal.*

Flegel, U., Vayssiere J. and Bitz, G. (2010), "A state of the art survey of fraud detection technology", *Insider Threats in Cyber Security,* Vol. 49, pp. 73-84.
Graham, L. and Bedard J.C. (2003), "Fraud risk and audit planning", *The International Journal of Accounting,* Vol. 7 No. 1, pp. 55-70.
Graham, J.R., Harvey, C.R. and Rajgopal, S. (2005), "The economic implications of corporate financial reporting", *Journal of Accounting and Economics,* Vol. 40 No. 1-3, pp. 3-73.
Hassink, H., Meuwissen, R. and Bollen, L. (2010), "Fraud detection, redress and reporting by auditors", *Managerial Auditing Journal,* Vol. 25 No. 9, pp. 861-881.
Healy, P.M. and Palepu, K.G. (2003), "The Fall of Enron", *Journal of Economic Perspectives,* Vol. 17 No. 2, pp. 3-26.
Hogan, C.E., Rezaee, Z., Riley Jr., R.A. and Velury, U.K. (2008), "Financial statement fraud: Insights from the academic literature", *Auditing: A Journal of Practice and Theory,* Vol. 27 No. 2, pp. 231-252.
Hylas, R.E. and Ashton, R. (1982), "Audit detection of financial statement errors", *The Accounting Review,* Vol. 57 No. 4, pp. 751-765.
Ivancevich, J.M., Duening, T.N., Gilbert, J.A. and Konopaske, R. (2003), "Deterring white-collar crime", *The Academy of Management Executive,* Vol. 17, pp. 114-127.
John, B., Jabber, B., & Sudharshan, V. (2012), "A study on Credit Card Fraud Detection Methods using Genetic Algorithm", *IJECCE*, Vol. 3 No. 3, pp. 413-415.
Johnson, G.G. and Rudesill, C.L. (2001), "An investigation into fraud prevention and detection of small businesses in the United States: Responsibilities of auditors, managers, and business owners", *Accounting Forum,* Vol. 25 No. 1, pp. 56–78.
Kakis, F.J. (1992), "Combating insurance fraud with forensic science", *Risk Management,* Vol. 39 No. 12, pp. 34-40.
Kaplan, R.L. (1987), "Accountants' liability and audit failures: When the umpire strikes out", *Journal of Accounting and Public Policy,* Vol. 6 No. 1, pp. 1-8.
Kaplan, S.E., Pope, K.R. and Samuels, J.A. (2010), "The effect of social confrontation on individuals' intentions to internally report fraud", *Behavioral Research in Accounting,* Vol. 22 No. 2, pp. 51-67.
Knapp, C.A. and Knapp, M.C. (2001), "The effects of experience and explicit fraud risk assessment in detecting fraud with analytical procedures", *Accounting, Organizations and Society,* Vol. 26, pp. 25-37.
Krummeck, S. (2000), "The Role of ethics in fraud prevention: A practitioner's perspective", *Business Ethics: A European Review,* Vol. 9 No. 4, pp. 268-272.
Kulik, B.W., O'Fallon, M.J., and Salimath, M.S. (2008), Do competitive environments lead to the rise and spread of unethical behavior? Parallels from Enron", *Journal of Business Ethics*, Vol. 83, pp. 703-723.
Kvale, S. and Brinkman, S. (2009), *InterViews: Learning the Craft of Qualitative Research Interviewing,* Sage Publications, London.
Loebbecke, J.K., Eining, M.M., and Wilingham, J.J. (1989), "Auditors' experience with material irregularities: Frequency, nature, and detectability", *Auditing: A Journal of Practice and Theory* Vol. 8, pp. 1-28.
Lord, A.T. (2010), "The prevalence of fraud: What should we, as academics, be doing to address the problem", *Accounting & Management Information Systems,* Vol. 9 No. 1, pp. 4-21.
Lowe, D.J., Reckers, P.M.J. and Whitecotton, S.M. (2002), "The effects of decision-aid use and reliability on jurors' evaluations of auditor liability", *The Accounting Review,* Vol. 77 No. 1, pp. 185-202.
Marcel, J. J., & Cowen, A. P. (2014), "Cleaning house or jumping ship? Understanding board upheaval following financial fraud", *Strategic Management Journal*, Vol. 35 No. 6, pp. 926-937.
Marshall, M.N. (1996), "Sampling for qualitative research", *Family Practice,* Vol. **13** No. 6, pp. 522-525.
Marshall, C. and Rossman, G. (1999), *Designing Qualitative Research*, 3rd ed., Sage Publications, Thousand Oaks, CA.

Matsumura, E.M. and Tucker, R.T. (1992), "Fraud detection: A theoretical foundation", *The Accounting Review,* Vol. 67 No. 4, pp. 753-782.
McMillan, J.H. and Wergin, J.F. (2006), *Understanding and evaluating educational research,* 3rd ed., Pearson Education Ltd, Upper Saddle River, NJ.
Murphy, K.J. (1999), "Executive compensation", in Ashenfelter, O. and Card, D. (Ed.), *Handbook of Labor Economics,* Vol. 3, North Holland, Amsterdam.
Murphy, P. and Dacin, M.T. (2011), "Pathways to fraud: A psychological perspective", *Journal of Business Ethics*.
Myers, M.D. (2009), *Qualitative Research in Business & Management*. Sage Publications, London.
Myers, M.D. and Newman, M. (2007), "The qualitative interview in IS research: Examining the craft", *Information and Organization,* Vol. 17, pp. 2-26.
Narayanan, V.G. (1994), "An analysis of auditor liability rules", *Journal of Accounting Research,* Vol. 32, pp. 39-59.
Owusu-Ansah, S., Moyes, G.D., Oyelere, P.B., and Hay, D. (2002), "An empirical analysis of the likelihood of detecting fraud in New Zealand", *Managerial Auditing Journal,* Vol. 17 No. 4, pp.192-204.
Palmer, D. (2008), "Extending the process model of collective corruption", *Research in Organizational Behavior,* Vol. 28, pp. 107-135.
Pathria, A. (1999), "Advanced fraud detection", *Risk Management,* Vol. 46 No. 3, pp. 23-28.
Patterson, E. and Wright, D. (2003), "Evidence of fraud, audit risk, and audit liability regimes", *Review of Accounting Studies,* Vol. 8, pp. 105-131.
Patton, M.Q. (1990), *Qualitative evaluation and research methods,* 2nd ed., Newbury Park, CA: Sage.
Pearson, T.A. and Singleton, T.W. (2008), "Fraud and forensic accounting in the digital environment", *Issues in Accounting Education,* Vol. 23 No. 4, pp. 545-559.
Perri, F.S. and Lichtenwald, T.G. (2007), "A proposed addition to the FBI criminal classification manual: fraud-detection homicide", *The Forensic Examiner* Winter, pp. 18-30.
Perri, F.S. and Brody, R.G. (2011), "The Sallie Rohrbach story: Lessons for auditors and fraud examiners", *Journal of Financial Crime,* Vol. 18 No. 1, pp. 93-104.
Peterson, B.K. and Buckhoff, T.A. (2004), "Anti-fraud education in academia", *Advances in Accounting Education: Teaching and Curriculum Innovations,* Vol. 6, pp. 45-67.
Polkinghorne, D.E. (1989), "Phenomenological research methods", In Valle, R.S. and Halling, S. (Ed.), *Existential-Phenomenological Perspectives in Psychology: Exploring the Breadth of Human Experience*, Plenum Press, New York, NY, pp. 41-60.
PricewaterhouseCoopers (2009), November, *The Global Economic Crime Survey: Economic Crime in a Downturn.*
Public Company Accounting Oversight Board (PCAOB) (2005), *Consideration of Fraud in a Financial Statement Audit,* AU Section 316, www.pcaobus.org
Rabl, T. (2011), "The impact of situational influences on corruption in organizations", *Journal of Business Ethics,* Vol. 100, pp. 85-101.
Rabl, T. (2008), *Private Corruption and its Actors – Insights into the Subjective Decision Making Processes,* Pabst, Lengerich.
Rabl, T. and Kuhlmann, T.M. "Understanding corruption in organizations – Development and empirical assessment of an action model", *Journal of Business Ethics,* Vol. 82 No. 2, pp. 477-495.
Rezaee, Z. (2005), "Causes, consequences, and deterrence of financial statement fraud", *Critical Perspectives on Accounting,* Vol. 16 No. 3, pp. 277-298.
Rezaee, Z., Crumbley, D.L. and Elmore, R.C. (2004), "Forensic accounting education", *Advances in Accounting Education: Teaching and Curriculum Innovations,* Vol. 6, pp. 193-231.
Rossouw, G.J. (2000), "Defining and understanding fraud: A South African case study", *Business Ethics Quarterly,* Vol. 10 No. 4, pp. 885-895.
Rubin, H.J. and Rubin, I.S. (2005), *Qualitative Interviewing: The Art of Hearing Data,* Sage, Thousand Oaks, CA.

Sarens, G., & Abdolmohammadi, M. J. (2011), "Factors associated with convergence of internal auditing practices: Emerging vs developed countries", *Journal of Accounting in Emerging Economies*, Vol. 1 No. 2, pp. 104-122.
Scharff, M.M. (2005), "Understanding WorldCom's accounting fraud: Did groupthink play a role?" *Journal of Leadership and Organizational Studies,* Vol. 11 No. 3, pp. 109-118.
Schwartz, S.T. and Wallin, D.E. (2002), "Behavioral implications of information systems on disclosure fraud", *Behavioral Research in Accounting,* Vol. 14, pp. 197-221.
Seidman, I. (2006), *Interviewing as Qualitative Research,* Teachers College Press, New York, NY.
Sidak, J.G. (2003), *The Failure of Good Intentions: The WorldCom Fraud and the Collapse of American Telecommunications after Deregulation,* Vol. 20., *Yale Journal on Regulation*, 207-268.
Smith, R.G. (2008), "Coordinating individual and organizational responses to fraud", *Crime Law Soc Change,* Vol. 49, pp. 379-396.
Sutherland, E.H. (1949), *White-Collar Crime,* Dryden Press, New York, NY.
Vanasco, R.R. (1998), "Fraud auditing", *Managerial Auditing Journal,* Vol. 13 No 1, pp. 4-71.
Weatherford, M. (2002), "Mining for fraud", *IEEE Intelligent Systems,* Vol. 17 No. 4, pp. 4-6.
Wells, J.T. (2004), "New approaches for fraud deterrence", *Journal of Accountancy.*
Wilks, J.T. and Zimbelman, M.F. (2004), "Decomposition of fraud-risk assessments and auditors' sensitivity to fraud cues", *Contemporary Accounting Research,* Vol. 21 No. 3, pp. 719-745.
Wright, A. and Ashton, R. (1989), "Identifying audit adjustments with attention-directing procedures", *The Accounting Review,* Vol. 64 No. 4, pp. 710-728.
Zahra, S.A., Priem, R.L. and Rasheed, A.A. (2005), "The antecedents and consequences of top management fraud", *Journal of Management,* Vol. 31 No. 1, pp. 803-828.
Zimbelman, M.F. (1997), "The effects of SAS No. 82 on auditors' attention to fraud risk factors and audit planning decisions", *Journal of Accounting Research,* Vol. 35, pp. 75-97.