Asset Misappropriation Research White Paper for the Institute for Fraud Prevention

by Chad Albrecht, Mary-Jo Kranacher & Steve Albrecht

Abstract

In this paper we provide a general overview of asset misappropriation. We discuss the current state of academic and practical knowledge as it relates to asset misappropriation, including what we currently know about asset misappropriation, what research has been done in this area, what is currently missing from the research, and what additional resources are needed in order to continue to provide high quality research on this topic.

Introduction

Asset misappropriation schemes include those frauds in which a perpetrator employs trickery or deceit to steal or misuse an organization's resources. In these cases, specific assets of the organization are taken to directly benefit the individuals committing the fraud. Individuals committing asset misappropriation-type crimes may be: employees of an organization, customers or vendors of an organization, or could be individuals unrelated to the victim organization. The distinguishing elements of asset misappropriation, however, are that an organization's assets are taken through trickery or deceit, rather than by force. Furthermore, the "act" of asset theft, concealment, and conversion must all be present. Asset misappropriation frauds are generally divided into two

main categories: (1) the theft of cash and (2) the theft of non-cash assets. Misappropriation of assets may occur under different circumstances: (1) before they are recorded in the books and records of an organization (i.e. skimming), (2) while assets are currently held by the organization (e.g. larceny or misuse of equipment, inventory, supplies, cash, etc.), or (3) during the process of purchasing goods or services (e.g., billing, expense reimbursement, payroll schemes). In this final scenario, the organization pays for something it shouldn't pay for or pays too much for purchased goods or services. Research has shown that, of these three types of asset misappropriation, fraud involving purchases is, by far, the most common and expensive for organizations.

Asset misappropriation schemes most often involve theft of cash, although this is not always the case. In a recent study by the Association of Certified Fraud Examiners, approximately 85% of all asset misappropriation cases involved the misuse of cash (ACFE, 2008).

What We Currently Know About Asset Misappropriation

There has been little academic research in the area of asset misappropriation (most academic fraud studies have focused on financial statement fraud). As a result, much of the research on asset misappropriation has been conducted by professional organizations. For example, the Association of Certified Fraud Examiners publishes the "Report to the Nation on Occupational Fraud and Abuse" every two years; the most recent study was released in 2008. Deloitte LLP, PricewaterhouseCoopers, and KPMG also publish the results of their studies regarding fraud against organizations—the 2005-2006 Integrity Survey published by KPMG Forensic (KPMG, 2006) and the Global

Economic Crime Survey published by PricewaterhouseCoopers in 2007 (PricewaterhouseCoopers, 2007)—greatly enhance our overall knowledge of asset misappropriation. A few authors, such as Joseph T. Wells and W. Steve Albrecht have written extensively about fraud and contributed significantly to our overall understanding of this societal problem.

Asset Misappropriation Schemes

According to the 2008 *Report to the Nation on Occupational Fraud and Abuse,* asset misappropriation can be categorized according to different scheme types, including: skimming, cash larceny, fraudulent disbursements, and non-cash larceny and misuse (ACFE, 2008).

Skimming includes those acts where funds are taken by the perpetrator before the funds have been recorded in the organization's financial records. Skimming may occur at the point of sale, from receivables, or from refunds.

Cash larceny refers to fraudulent acts that involve the theft of funds after they have been recorded. The cash is typically stolen from the cash on hand, such as from the cash register or petty cash, or taken from a deposit.

Fraudulent disbursements cover a wide variety of schemes: 1) Billing schemes typically involve employers making payments based on false invoices for personal purchases; 2) Check tampering refers to altering or forging an organization's check for personal use; 3) Expense reimbursements include false claims of fictitious business expenses; 4) Payroll schemes resemble billing schemes in that payment is based on false documentation, such as timecards, which indicated that compensation is fraudulently due to an employee; and 5)

Cash register disbursements entail false entries or "no sale" transactions to hide the removal of cash.

Finally, non-cash misappropriations involve those schemes where employees steal or misuse the non-cash assets of the organization, such as inventory or equipment, for their own personal benefit.

Some asset misappropriation frauds are large enough that they result in the material misstatement of the financial statements of the organization, without management's knowledge or intent to deceive. For example, a derivatives fraud committed by an employee of a Japanese company resulted in a $2 billion misstatement of that company's financial statements, and a purchasing fraud against a U.S. auto maker resulted in a more than $400 million misstatement of its financial statements. Both of these frauds had a material effect on the financial statements, yet were unknown to management, as is the case in many asset misappropriation schemes (O'Keefe, Wambsganss, and Dosch, 2006). While auditors are generally more concerned about financial statement misstatements than they are about asset misappropriation, large asset misappropriations can potentially threaten the economic well being of an organization.

A Serious Problem

Unfortunately, asset misappropriation is a major problem for organizations throughout the world. Some research has even suggested that organizations lose as much as 7% of annual revenues to frauds such as asset misappropriation (ACFE, 2008). To better understand the consequences that

asset misappropriation pose to an organization, consider the following: A few years ago, a U.S. automobile manufacturer was the victim of a large asset misappropriation scheme. Because fraud reduces a firm's income on a dollar-for-dollar basis, the company's bottom line was reduced by the total fraud loss of approximately $436 million. As a result, much more additional revenue is needed to restore net income to what it would have been without the theft, than merely the amount of the actual fraud loss. Assuming that the automobile manufacturer's profit margin (net income divided by net sales) was 10 percent, the company would have to generate up to $4.36 *billion* in addition revenue. In other words, to make up for the cost of the fraud the company would have to have additional revenues of approximately ten times the cost of the fraud to restore the effect that the fraud had on net income. If we assume that the company has an average selling price of $20,000 per car, the company would have to produce and successfully sell 218,000 cars to make up for the $436 million fraud loss.

When an asset misappropriation takes place, there are no winners. The perpetrators are almost always caught and suffer personal and professional embarrassment, loss of job and career, and legal consequences. Perpetrators are also often forced to make tax and restitution payments. Victims lose because, in addition to having their assets stolen, they incur legal fees and experience negative publicity. Often, the culture and morale of the organization is adversely affected, resulting in lost productivity, increased employee turnover and absenteeism.

The Nature of Asset Misappropriation

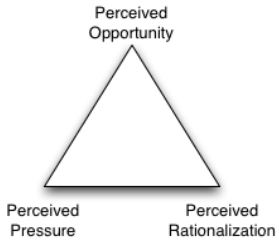
Asset misappropriation schemes generally start small and get larger as perpetrators gain confidence in their ability to get away with their dishonest schemes. While events, such as an internal or external audit, may threaten the perpetrator's attempts at concealment and cause the scheme to be discontinued for a period of time, once the threat has passed, the perpetrator(s) will typically resume the scheme and continue to steal until the fraud is detected. Since the dollar amount of the scheme almost always increases with time, the amount a perpetrator steals in the last few days or months of the fraud tends to greatly exceed the average amount taken during the earlier periods of the scheme.

Classical fraud theory provides an excellent foundation to better understand the motivations for asset misappropriation. This theory states that in order for asset misappropriation to take place, the perpetrator must: 1) be experiencing a perceived pressure, 2) have a perceived opportunity to commit the fraud, and 3) find a way to rationalize his or her actions as acceptable.

While most pressures often involve a perceived financial need, perceived non-financial pressures, such as the need to report better than actual performance, frustration with work, or even a challenge to beat the system, can also motivate fraud,

The opportunity involves the belief that the perpetrator can commit the fraud and not get caught or if he or she does get caught, nothing serious will happen. These opportunities don't have to be real; they must only appear to be real to the perpetrator. This explains why the mere perception of detection acts as a deterrent to fraud.

Common rationalizations include, “I’m only borrowing and will pay it back,” “it’s only for a short period of time,” “it’s not hurting anyone,” or “they owe me.” The three elements of the fraud triangle are essential to any type of asset misappropriation scheme and are presented below.



In 1949, Edwin Sutherland, a criminologist at the University of Indiana identified many differences between street crime and what he later described as “white-collar” crime. Such differences included a violation by a person in a position of trust in professions such as medicine, law, accounting, business, and banking. In addition, white-collar crime is typically committed by those of high status and power. The research and theories that Sutherland developed have become the basis for much of the research currently conducted on organizational and occupational fraud and abuse.

Donald Cressey, one of Sutherland’s most successful students, took this idea a step further by identifying three conditions, all of which must be present if embezzlement is to take place. These three conditions include: 1) financial problems defined as non-sharable, 2) an opportunity to violate trust, and 3) the rationalization of the act.

Later, Albrecht, Romney, Cherrington, Paine, and Roe introduced the ideas by Sutherland and Cressey into business literature. These researchers further suggested that the three elements of the fraud triangle were interactive and need not be real, only perceived to be real by the perpetrator(s). They determined that if one factor was weighted more heavily, less of the other factors needed to exist for fraud to occur.

How People are Recruited to Participate in Asset Misappropriation

The Report to the Nation by the Association of Certified Fraud examiners suggested that in roughly two-thirds of fraud cases, the perpetrator acted alone. However, when collusion was involved, the median loss to the organization is four times higher than the amount lost to perpetrators who acted alone. Recent research by Albrecht et al (2008), suggests that multiple individuals become involved in asset misappropriation schemes as a result of power that is exerted by the initial perpetrator on potential collaborators.

This research also found that once an individual began to commit asset misappropriation, he or she then recruited others to participate in the scheme on an as-needed basis. Based upon this finding, the initial perpetrator of the fraud may exercise one or more of the five types of power as described by French and Raven (1959) on potential conspirators. These five types of power include: reward, coercive, legitimate, referent, and expert power.

Reward power is the ability of a fraud perpetrator to convince a potential victim that he or she will receive a certain benefit through participation in the fraud scheme. Examples of such rewards may include a cash payment, a large

bonus, or even job promotion. Coercive power is the ability of the initial perpetrator to make a potential conspirator perceive punishment if he or she does not participate in the asset misappropriation scheme. Examples of punishments that individuals may fear by not participating in a fraudulent scheme may include public humiliation, whistle-blowing fears, or even job loss. Expert power deals with the ability that the perpetrator may have to influence others based upon the perpetrator's expert knowledge. Individuals who are influenced by this type of power may not even be aware that an asset misappropriation scheme is taking place and may do things that enable the perpetrator simply because the victim believes the perpetrator is an honest person who knows more about the policies and procedures that the victim does. Legitimate power is based on authority. For example, the head of the accounting department within an organization may claim to have legitimate power to make decisions and lead the organization – even if that direction is unethical. In such situations, the accounts payable clerk may sign a check just because someone in authority has asked him or her to do so. Finally, referent power refers to the perpetrator's ability to relate, on a personal level, with the potential victim. In this type of situation, many individuals, when asked to participate by a trusted friend, will rationalize the acts as being justifiable.

By understanding how perpetrators use power to recruit and persuade others to participate in asset misappropriation schemes, it is possible to better understand how frauds can grow and eventually involve many people. The effectiveness of the perpetrator to influence potential conspirators depends largely on the susceptibility of the potential conspirator to the various types of

power. Similar to the fraud triangle, the five types of power are interactive, meaning that the more susceptible a potential conspirator is to the various types of power, the less of the other types of power are needed to recruit the potential conspirator to participate in the scheme.

Organizations with Weak Internal Controls

Prior research suggests that organizations with weak internal controls are especially susceptible to fraudulent asset misappropriation schemes (KPMG, 2004). International control weaknesses include: a lack of segregation of duties, physical safeguards, independent checks, proper authorization, proper documents and records (all internal control activities); overriding existing controls; and an inadequate accounting system. Many studies have found that overriding existing internal controls creates the greatest opportunity for asset misappropriation schemes (Albrecht, 2008).

A good system of internal controls will help to deter and prevent asset misappropriation schemes from occurring within organizations (Holtfreter, 2004). The Institute of Internal Auditors (IIA) has even recommended that auditors have a responsibility to assist management with the evaluation of internal controls that are used to detect and mitigate fraud (Institute of Internal Auditors, 2007). In order to prevent asset misappropriation schemes and similar types of fraud from occurring within organizations, the Committee of Sponsoring Organizations (COSO, 1992) has suggested that an internal control framework should include (1) a good control environment, (2) a good accounting system, (3) good control activities, (4) monitoring, and (5) good communication and information.

Who Commits Asset Misappropriation?

Research by the Association of Certified Fraud Examiners has found that individuals involved in fraud, including asset misappropriation schemes, have many common characteristics (ACFE, 2008). For example, men are twice as likely to commit fraud as females. This research corresponds to other business ethics research that suggests women are typically more ethical than men (Ibrahim and Angelidis, 2008; Marta, Singhapakdi, and Kraft, 2008). Similarly, individuals who participated in fraud are most likely to be between the ages of 41 – 50 years old. In the 2008 ACFE study, for example, more than half of all perpetrators were over forty years old. Most fraud perpetrators have attended or graduated from college and many perpetrators have obtained a post-graduate degree. In general, the higher the education level of the individual, the more costly the scheme is to the organization. Individuals involved in fraudulent schemes tend to live beyond their means and struggle with financial difficulties. Fraud perpetrators often have a "wheeler-dealer attitude" and many refuse to take vacations from work. Finally, many fraud perpetrators have personal problems and exhibit signs of irritability and defensiveness.

While the recent ACFE study helps to better identify the types of individuals who are involved in fraudulent asset misappropriation schemes, research has also shown that essentially anyone can commit fraud. As a result, it is very difficult to distinguish perpetrators of fraud based on demographic or psychological characteristics. In one study, for example, fraud perpetrators were compared to (1) prisoners incarcerated for property offenses, and (2) a sample of noncriminal, college students. While the results of the study showed that the

three groups are different, it found that when fraud perpetrators were compared to incarcerated prisoners, fraud perpetrators were very different. Those involved in fraud tended to be much more religious, better educated, less likely to have a criminal record and less likely to use drugs. On the other hand, when fraud perpetrators were compared to college students, the characteristics, while different, bore some similarities. For example, both the perpetrators and college students were well-educated, expressed social conformity, exhibited self-control, and showed empathy to others (Romney, 1980).

Prevention of Asset Misappropriation

Since everyone loses once an asset misappropriate fraud has occurred, organizations can realize huge savings through fraud prevention. Most organizations have some preventive controls in place, but realize that, even the best controls, cannot prevent all frauds. As was shown with the fraud triangle, anyone with perceived pressure, opportunity, and an ability to rationalize their crime, can commit fraud. Therefore, organizations should engage in pro-active fraud prevention, regardless of how honest they believe their employees are.

Fraud prevention is another area where there has been little academic research. What we do know is that the major elements of fraud prevention are (1) creating a culture of honesty, openness and assistance for all employees and, (2) eliminating opportunities for fraud to occur.

Creating a culture of honesty, openness and assistance usually involves the following elements: (1) hiring honest people and providing fraud awareness

training, (2) creating a positive work environment, and (3) implementing effective employee assistance programs (EAPs).

Eliminating fraud opportunities generally include: (1) maintaining a good system of internal controls, (2) implementing ways to discourage collusion between employees and others, (3) alerting vendors, customers and contractors to company purchasing and sales policies, (4) monitoring employees and instituting an effective whistle-blower system, (5) creating an expectation of enforcement within the organization, and (6) conducting pro-active fraud auditing.

Each of these elements deserves additional research and is an important area for future study. While very little academic research has been done by business researchers on these topics, there has been related academic work by behavioral researchers that could be leveraged to help us understand how to effectively carry out these fraud prevention measures. Indeed, fraud prevention could be a very fruitful area of academic research, including the separate study of each of these elements or the intersection of how these elements contribute to reducing fraud and other counter-productive acts (e.g. discrimination, safety issues, substance abuse, etc.) within organizations.

Fraud Detection

Like fraud prevention, fraud detection is an exciting area for future academic research. Currently, fraud detection techniques involve identifying and following-up on fraud symptoms, or red flags, to determine if they are forewarning of real fraud (Seetharaman, Senthilvelmurugan, and

Periyanayagam, 2004). The red flags for asset misappropriation fall into six categories:

(1) accounting anomalies, such as faulty journal entries, inaccuracies in ledgers, or fictitious documents,

(2) internal control overrides and breakdowns,

(3) analytical fraud symptoms, which include procedures or relationships that are unusual or too unrealistic to be plausible, for example, transactions or events that happen at odd times or places; that are performed by or involve people who would not normally participate; or that include odd procedures, policies or practices. They might also include transaction amounts that are too large or too small. Basically, analytical symptoms represent anything out of the ordinary),

(4) lifestyle symptoms (people who commit fraud usually meet their immediate need and then gradually start to increase their lifestyles),

(5) unusual behaviors (people who are involved in fraud often feel stress and, as a result, change their behaviors to cope with this stress), and

(6) tips and complaints that something is suspicious.

Academic research could be conducted to determine if there are other categories of symptoms in addition to the ones already mentioned, and how each of these symptoms becomes apparent when individuals commit fraud. Cross-cultural studies could be conducted to determine if asset misappropriation

symptoms are the same across different cultures as well as which asset misappropriation symptoms are most prominent in certain cultures.

In addition to understanding the nature of fraud symptoms, the best academic research would determine how to pro-actively search for these symptoms. Such research could include predictive models that would combine the various symptoms into usable detection techniques. The most promising area of fraud detection research is the use of technology to search for fraud symptoms and red flags. Data analysis, such as data mining, strategic fraud detection, and other technology applications, presents exciting research opportunities. While advances in technology have made fraud easier to commit (also a good research topic), technology has also made fraud easier to detect. Future research in this area could help us to analyze and understand business functions, and the various kinds of frauds that could occur in each function. Furthermore, future research could also use technology to identify the symptoms exhibited by each of these frauds and pro-actively search for them. Consequently, we would be able to catch frauds in the early stages.

Investigation of Fraud

Of these three fraud elements—prevention, detection and investigation—more resources have been spent on the investigation aspects than prevention or detection. Many fraud investigation methods examine the "act," the concealment, or the conversion elements of fraud. Some of these methods include surveillance and covert operations, invigilation, gathering physical, documentary, or electronic evidence, using forensic software tools to capture electronic information, searching public and private databases and Internet sites,

using the net worth method to determine unsupported spending and various types of interviewing techniques.

Each of these topics deserves additional academic research. Most fraud investigations are conducted by individuals trained in law enforcement, not business. Usually, these investigators have more experience with investigating property and street crimes, and are not familiar with the nuances of fraud. Research that brings traditional investigative techniques to investigations of fraud while taking into account the special nature of white collar crime could potentially yield very fruitful results. Additionally, research that identifies the most efficient and effective investigation methods and the best investigative sequence for different types of frauds could also be beneficial. Each year, hundreds of millions of dollars are spent on fraud investigation, when effective prevention and better investigative techniques could reduce these expenditures considerably.

Follow-up on Fraud and Fraud Perpetrators

Another area of potential research is learning how to effectively deal with fraud perpetrators and their organizations once fraud has been discovered and investigated. Most organizations do not prosecute perpetrators; rather, they quietly dismiss them without any civil or criminal action to avoid the bad press that accompanies the prosecution of the perpetrator. Research that combines fraud knowledge with criminology research could be performed to determine the best follow-up actions to take when fraud has been detected. We need to learn more about the affects on the organization and employees that not pursuing civil and/or criminal actions might have. Does the lack of prosecution

encourage others to commit fraud? How should the details of a fraud be communicated throughout an organization so that employees will know that the organization doesn't take fraud lightly? Are there any circumstances under which it is not effective to prosecute a perpetrator? When should civil action be taken? What can be done to change the organization culture to prevent similar frauds in the future? There are many research questions involving organizational and individual follow-up once fraud has occurred.

Fraud Statistics and Frequency of Occurrence

While great strides have been made in recent years to better understand asset misappropriation, we still don't know some basic facts regarding asset misappropriation schemes. This includes the prevalence of asset misappropriation, its effect on organizations throughout the world, the effectiveness and pervasiveness of proactive asset misappropriation detection techniques, and the impact of contextual, environmental, and cultural factors on this problem. Statistically valid empirical research is urgently needed to support future efforts to mitigate asset misappropriation.

Statistics on asset misappropriation come from four basic sources: victim organizations, insurance companies, government agencies and researchers. Understandably, victim organizations typically attempt to put the fraud behind them as quickly as possible. In order to minimize public exposure and embarrassment, they generally do not make the fraud public or prosecute the perpetrator (Bussmann and Werle, 2006). As a result, obtaining accurate asset misappropriation statistics from victim organizations is difficult.

Many insurance companies provide fidelity bonding or other types of coverage against asset misappropriation and often provide related statistics. However, these statistics only correspond to the actual cases where the insurance company provided employee bonding or other insurance – creating an incomplete picture.

Government agencies, such as the IRS, FDIC, and FBI, often provide fraud statistics, but these agencies only provide statistics based on their jurisdictions. These statistics are often not collected randomly, may not be complete, and do not provide enough information to fully understand asset misappropriation (Levi and Burrows, 2008).

Finally, while researchers attempt to collect data about asset misappropriation in various industries, they have a difficult time getting complete data regarding actual fraud losses.

Unfortunately, the majority of studies on asset misappropriation have been contained to the United States, England, Australia, and other developed countries. While this research has given us some information on asset misappropriation in general, we still don't fully understand the extent of this type of fraud in many countries throughout the world. This is especially true for developing and under-developed nations, as a result of the lack of dependable data.

Recent cross-cultural research on business ethics has suggested that whether an act is considered to be ethical or not depends entirely upon the culture of the individuals participating in that act. As such, many acts that are

considered to be unethical under western standards are considered be acceptable and even ethical in some developing companies. For example, in most western countries, taking company assets, such as trade secrets or patents, is considered to be a serious crime and completely unethical; however, the same may not be true in some third-world countries.

Additional Resources Needed For Asset Misappropriation Research

Our understanding and knowledge of asset misappropriation would be greatly enhanced if there was increased interest by the academic community to study asset misappropriation using sound experimental, empirical, and other scholarly research methods. Such research would include developing and testing current theories, as well as applying rigorous methodologies to the various elements of asset misappropriation. Similarly, our understanding of this topic would be greatly enhanced if organizations made their asset misappropriation data available to researchers. This could potentially be achieved through a self-reporting fraud database, where organizations could anonymously report their data involving asset misappropriation and other types of fraud, which would then be made accessible to researchers.

Finally, organizations need to formally assign someone within their organizations to take responsibility for preventing, detecting, and investigating asset misappropriation (Hillison, Pacini, Sinason, 1999). By assigning formal responsibility for this function, these individuals could take proactive measures to reduce fraud within the organization. Furthermore, educational resources would become more widely available within the organization.

Conclusion

In conclusion, asset misappropriation is a very expensive problem for organizations. Unfortunately, few organizations proactively address this problem, which creates a reoccurring cycle of theft within many organizations. By creating a proactive asset misappropriation policy, organizations can effectively assign responsibility and greatly reduce their susceptibility to these schemes.

Asset misappropriation could provide a fertile area of research for practitioners, academics, governmental entities, and others. While the last 50 years have greatly enhanced our overall understanding of asset misappropriation, we still lack knowledge of some of its basic characteristics. Specific areas of interest include asset misappropriation in international organizations, the effects of culture on this type of fraud, and proactive detection and prevention procedures. Finally, future research into asset misappropriation must include longitudinal studies that help us better understand how an organization's susceptibility to asset misappropriation schemes varies depending on the state of the economy, the lifecycle of the organization, the organizational culture, and the organization's industry.

It is our hope that the next few years will bring greater knowledge and understanding to the problem of asset misappropriation. As with all types of fraud, education and research is the key to its deterrence. When the fraud examination community fully understands the nature of asset misappropriation, we will be able to better design programs, tools, and methods to minimize its occurrence within organizations.

References:

AICPA, *Statement on Auditing Standards #82*: *Consideration of Fraud in a Financial Statement Audit* (New York: AICPA, 1997).

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

Albrecht, W. Steve, K. R. Howe, and M. B. Romney, *Detecting Fraud: The Internal Auditor's Perspective*, Maitland, FL: The Institute of Internal Auditors Research Foundation, 1982.

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

Bussmann, Kai-D and Markus M. Werle, 2006, *Addressing Crime in Companies – First Findings from a Global Survey of Economic Crime*, The British Journal of Criminology, Volume 46, Issue 6, pages 1128 – 1144.

French, J.R.P., Jr. and B. Raven, "The Basis of Social Power," in D. Cartwright, Ed., *Studies in Social Power* (Ann Arbor, MI: University of Michigan Press).

Hillison, William, Pacini, Carl, and Sinason, David, 1999, The Internal Auditor as a Fraud-Buster, *Managerial Auditing Journal,* Volume 14, Issue 7, pages 351 – 363.

Holtfreter, Kristy, 2004, Fraud in US Organizations: An Examination of Control Mechanisms, Volume 12, Issue 1, pages 88 – 95.

Ibrahim, Nabil and John Angelidis, The Relative Importance of Ethics as a Selection Criterion for Entry-Level Public Accountants: Does Gender Make a Difference?, Journal of Business Ethics (forthcoming).

Institute of Internal Auditors, 2007, "Internal Audit Facts," *About-the-Profession*, Available at http://stage.theiia.org/theiia/about-the-profession/internal-audit-facts/?i=3087.

KPMG, 2004, *Fraud Survey 2003*, Montvale, NJ, USA.

KPMG, 2006, *Integrity Survey 2005 – 2006*, NJ, USA.

Levi, Michael and John Burrows, 2008, Measuring the Impact of Fraud in the UK – A Conceptual and Empirical Journal, British Journal of Criminology, Vol. 48, Issue 3, pages 293 – 318.

Marta, Janet, Singhapakdi, Anusorn, and Kenneth Kraft, 2008, "Personal Characteristics Underlying Ethical Decisions in Marketing Situations: A Survey of Small Business Managers," Journal of Small Business Management, Volume 46, Issue 4, pp. 589 – 606.

O'Keefe, Timothy Paul, Wambsganss, Jacob R, and Robert J. Dosch, 2006, Examining for Fraud: A Case for a Larger Alpha, *Journal of Forensic Accounting*, Volume 7, pages 1 -16.

PricewaterhouseCoopers, 2007, Economic Crime: People, Culture and Controls, Global Economic Crimey Survey 2007, London, England.

Romney, Marshal B., Albrecht, W. S., and Cherrington, David. J. (1980), "Red-Flagging the White-Collar Criminal," *Management Accounting*, March, 51 – 70.

Seetharaman, A., Senthilvelmurugan, V. and Rajan Periyanayagam, 2004, Anatomy of Computer Accounting Frauds, *Managerial Auditing Journal*, Volume 19, Issue 8, Pages 1055 – 1072.

Wells, Joseph, 1997, Occupational Fraud and Abuse, Obsidian Publishing Company, Austin: TX.