WHEN IS COMPUTERIZED CONTINUOUS AUDITING LESS EFFECTIVE AT DETERRING FRAUD?

by

George C. Gonzalez

B.S. in Accounting, University of Florida, 1980

Submitted to the Graduate Faculty of

Joseph M. Katz Graduate School of Business in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

UNIVERSITY OF PITTSBURGH

Joseph M. Katz Graduate School of Business

This dissertation was presented

by

George C. Gonzalez

It was defended on

July 17, 2012

and approved by

Jacob G. Birnberg, Professor Emeritus, Katz Graduate School of Business

Dennis F. Galletta, Professor, Katz Graduate School of Business

Kevin H. Kim, Associate Professor, School of Education

Donald V. Moser, Professor, Katz Graduate School of Business

Vicky B. Hoffman (Chair), Professor, Katz Graduate School of Business

WHEN IS COMPUTERIZED CONTINUOUS AUDITING LESS EFFECTIVE AT DETERRING FRAUD?

George C. Gonzalez, PhD

University of Pittsburgh, 2012

Companies use a variety of techniques to deter fraudulent behavior. This study focuses on the fraud deterrent effect of computerized continuous auditing systems. Although continuous auditing systems are almost always computerized in the natural environment, this study reports the results of two experiments that separately examine the effects of continuous versus periodic auditing and manual versus computerized fraud detection. It also examines the relative effects of human versus computer-mediated communication of the audit findings. Consistent with theory from criminology, information systems, and psychology, I find that the effectiveness of a continuous audit approach depends on the actual probability of fraud detection, and that at low levels of fraud detection a continuous audit is actually less effective than a periodic audit in reducing the perceived opportunity to commit fraud. I find no differences based on whether fraud is detected by a manual or computerized system, but find moderate support that face-to-face communication of audit findings creates more discomfort in a potential fraud perpetrator than does computer-mediated feedback. Contrary to my predictions, I do not find that individuals' perceptions translate into corresponding effects on actual fraudulent behavior in my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1.0 INTRODUCTION

This study focuses on the fraud deterrent effect of computerized continuous auditing systems. Although continuous auditing systems are almost always computerized in the natural environment, this study uses the comparative advantages of the experimental method to separately examine effects that often co-occur in the real world. In this way, I can determine which aspects of a system are effective at deterring fraud. Specifically, the study examines the relative effectiveness at deterring fraud of a continuous versus periodic auditing system (i.e., audit frequency), a computerized versus manual fraud detection system (i.e., system mode), and whether audit results are communicated by a human in a face-to-face interaction or by a computer (i.e., communication feedback mode). This study also tests whether continuous auditing's effectiveness as a fraud deterrent depends on the actual fraud detection probability. Most contemporary audit literature assumes that because continuous auditing is a constant, persistent presence, it will always be more of a fraud deterrent than periodic auditing. While continuous auditing could be more effective as a fraud deterrent than periodic auditing when the actual probability of fraud detection is high, I predict that continuous auditing will be less effective than periodic auditing when there is a low actual probability of fraud detection.

Because traditional paper-based audit trails are steadily disappearing and being replaced by digital audit evidence, auditors are increasingly relying on computerized audit techniques to

gather digital evidence. Computers are being used by organizations seeking to "do more with less" by reducing staff, including internal audit staff, while attempting to increase audit efficiency through information technology. Although fraud deterrence is a top priority for auditors, firms, and regulators, little is known about computerized continuous auditing's effects on fraudulent behavior. It is important to understand whether moving from a manual periodic audit environment to a computerized continuous audit environment affects the behavior of auditees, and to determine which aspects of this process influence a potential fraud perpetrator's perceptions and behavior. This study extends the limited prior research in this area.

To answer my research questions, I conduct a two-experiment study in which participants perform an auditable task under different conditions. Participants perform the task for compensation across repeated periods. In some cases, randomly determined, participants can increase their compensation by performing the task fraudulently (i.e., in an opportunistic, dishonest manner) provided this behavior is not detected through an audit. I examine the effect on perceived opportunity to commit fraud and on actual fraud behavior of manipulating the audit frequency, the system mode, the communication feedback mode, and the actual audit detection probability. The intent of varying these factors is to isolate their deterrent effects based on participants' perceptions of the likelihood that they will be detected behaving fraudulently. In my first experiment I vary the probability of getting audited to examine the interaction between audit frequency and actual detection probability. In the second experiment I hold audit frequency and actual detection probability constant as I observe the deterrent effects of varying the system mode and the communication feedback mode. In all circumstances, when a participant is audited, the fraud is detected, i.e., in this study all audits are 100% successful in detecting fraud and therefore the actual audit detection probability is the same as the probability of being audited.

Participants who commit fraud earn additional compensation unless they are audited, in which case their fraud is detected and they pay a penalty which results in negative earnings for the period.

In the next chapter I present the background for my study, including a discussion of fraud, auditing, human-computer interaction and other related issues. In Chapter 3 I discuss theory and develop my hypotheses. I describe my research method in Chapter 4 and the results of my experiments in Chapter 5, then summarize and conclude in Chapter 6.

2.0 BACKGROUND AND MOTIVATION

2.1 THE IMPORTANCE OF FRAUD

Fraud is extremely costly. According to the Association of Certified Fraud Examiners (ACFE), the typical organization loses 5% of its annual revenue to fraud (ACFE 2012), which translates to a potential total fraud loss of more than $3.5 trillion worldwide when applied to the estimated 2011 Gross World Product (ACFE 2012). The median loss caused by occupational frauds (i.e., asset misappropriation, financial statement fraud, and corruption) during the two year period from January 2010 to December 2011 was $140,000 per organization (ACFE 2012), and more than one-fifth of those fraud losses were $1 million or more (ACFE 2012).[1] Auditors, managers, investors and regulators in businesses and industries of all types are concerned with the risk of fraud, and want to know how to most effectively minimize this risk.

While fraud has likely existed for as long as humans have engaged in transactions with one another, in the last decade it has received a great deal of attention. This attention is due to several key factors. One is the highly publicized fraud scandals at the beginning of the 21st

[1] According to the ACFE's 2012 Report to the Nations, among the three main categories of fraud, the median loss (percentage of cases) during the two-year period ended December 31, 2011 were: (1) asset misappropriation - $120,000 (86.7%); (2) financial statement fraud - $1 million (7.6%); and (3) corruption - $250,000 (33.4%). Note: the sum of percentages exceeds 100% because several cases involved schemes from more than one category. (ACFE 2012)

century, particularly those at Enron and Worldcom, which affected millions of investors and employees. Another important factor is the continual rise in use of information technology and the resulting increase in the variety of ways that fraud may be perpetrated. Advances in information technology represent a double-edged sword that simultaneously provides greater fraud-fighting tools while introducing new fraud risks. A complete database search for specific names or keywords among thousands of records can be done in a matter of seconds. Queries can be done on the frequency, dates, and/or times of day that an employee accesses a certain system. The matching of fields among different records, e.g., matching customer ship-to addresses to employee payroll addresses, can be done instantly. These types of data searches serve as fraud detection techniques and, by their known existence on the part of potential fraud perpetrators, as fraud deterrence tools.

On the other hand, technological advances create new types of fraud risk. For example, technology has made it easier for perpetrators to commit document fraud. Many types of documents of value, such as commercial checks, birth certificates, identification cards, licenses, motor vehicle titles, prescriptions, college transcripts, tickets and passes for events, are at risk of being forged (e.g., Zellen 2008). Another example of increased fraud risk spawned by advanced technology is in e-commerce (e.g., Shih et al. 2005). While e-commerce has given merchants access to much greater numbers of markets and customers around the world than they previously had, it has also introduced new fraud risks. One of the fraud risks associated with e-commerce is the risk that hackers will infiltrate a web page that customers use to order products online. A successful hacker could redirect a shipment of product to an alternative address, or gather the customer's credit card and other personal information and use that information to place fraudulent online orders elsewhere. Fraudsters steal credit card information in a variety of other

ways, such as through the use of hand-held credit card skimmers at restaurants and other establishments, and through hidden camera skimming devices at bank ATM machines (e.g., Nussenbaum 2010).

Because of its costliness, the high level of attention it has garnered, and the expanded risks associated with it as a result of technological advances, fraud is an issue of high importance to auditors, managers, investors and regulators.

2.2 THE ROLE OF AUDITORS

Both external auditors and internal auditors are concerned with fraud. External auditors must follow Public Company Accounting Oversight Board (PCAOB) auditing standards (AS) and American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) that require them to consider fraud in performing their audits of public companies.[2] Internal auditors, who act as a fraud deterrent and fraud detection mechanism, and are a key component of an internal control system (San Miguel & Govindarajan 1984), are subject to the Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF) standards that refer to fraud.[3] In general, both external and internal audit standards require that auditors be aware of fraud risk, incorporate fraud risk assessments into their audit engagements, and develop audit plans in accordance with those assessments.

---

[2] AS Nos. 1, 3, 4, 5, 6 and 7 explicitly mention fraud http://pcaobus.org/Standards/Pages/default.aspx; SAS No. 99 (AICPA 2002) is dedicated exclusively to fraud consideration in the performance of a financial statement audit, and requires brainstorming about fraud risks and potential fraud schemes.

[3] See IIA Standards 1200, 1220, 2060, 2120 and 2210 (IIA 2209a).

While external auditors are principally concerned with the detection of fraud that results in materially misstated financial statements (e.g., AICPA 2002), internal auditors typically view fraud risk more broadly and are concerned with fraud risks related to not only financial reporting but also compliance matters and operational effectiveness and efficiency (IIA 2009d). Accordingly, internal auditors generally tend to be equally concerned with fraud in all three of the ACFE's fraud categories (i.e., asset misappropriation, financial statement fraud and corruption), and engage in both fraud detection and fraud deterrence measures. Thus, this study should be of interest to auditors of all types, but should be of particular interest to internal auditors.

2.3 THE FRAUD TRIANGLE

Often-cited in the fraud literature is the concept of the fraud triangle, which consists of three conditions generally present when fraud occurs: perceived opportunity, incentive/pressure, and attitude/rationalization. Both academic (e.g., Hogan et al. 2008; Wilks and Zimbelman 2004a, 2004b) and practice-oriented (e.g., Wells 2001; Wells 2010) fraud literature use the fraud triangle to conceptualize the factors that are conducive to fraudulent behavior. In addition, the fraud audit standard (SAS No. 99) is based on the fraud triangle.

The fraud triangle is the conceptual framework upon which anti-fraud programs are frequently built. Because organizations usually have more control over the opportunity side of the fraud triangle than the other two sides (e.g., Albrecht et al. 2008; Albrecht et al. 2012; Wells 2010), most anti-fraud controls focus on minimizing fraud opportunities by deterring fraud

before the fact and detecting fraud after the fact. Successful fraud deterrence occurs when the potential perpetrator perceives a high certainty that he cannot commit a fraudulent act without it (1) being detected by the system of internal controls and (2) resulting in a penalty that outweighs any perceived potential benefits from the fraud. An example of a fraud deterrence tool that has proven successful for many businesses is the installation of replica (fake) surveillance cameras. The cameras are strategically positioned to give the appearance to customers and/or employees that they are being watched and recorded, thereby creating an (artificially) high probability of detection and deterring potential perpetrators from engaging in fraudulent behavior (e.g., Jans et al. 2010).

2.4 EVOLVING AUTOMATION OF AUDIT TECHNIQUES

The traditional audit is “manual”. It is based on the auditor performing face-to-face interviews, on-site observations, and manual reviews of hard copy (paper-based) audit evidence. A department or business unit within an organization would typically be subject to an audit on a periodic basis unless there was a special need for an immediate audit. An auditee could anticipate a visit from an external or internal auditor and being asked for specific pieces of documentation.

Since the early 1990s, the business environment has gone through substantial changes with the “electronization’’ of business, which has led to accounting systems that are less paper-based (e.g., Flowerday et al. 2006). The modern audit can be characterized as being “computerized,” where digital (electronic) evidence is gathered. Computerized audits, in whole

or in part, can be accomplished in many cases without the need for the auditor's physical presence at the auditee's office or other transaction source.

The evolution of computerized auditing techniques and the resulting replacement of traditional manual audits with computerized audits represent an evolution from a manual system, in which manually generated data are manually audited, to a computerized system, in which computer-generated data are audited by computer. My dissertation identifies three distinct dimensions of the evolution from manual to automated systems, and separately examines the ramifications of each of the three aspects. One aspect that I examine is whether a computerized system environment affects an auditee's inclination to commit fraud, as compared to a manual system environment. A second one is the effect of continuous auditing on auditee behavior, as compared to periodic auditing. The third aspect is communication of feedback.

Continuous auditing is a particular type of computerized audit that has gained growing interest. In a continuous audit, software continuously monitors transactions and compares their characteristics to expected results. Continuous auditing differs from traditional, man-powered auditing in several important ways. Continuous auditing (a) is designed to immediately detect and deter problems, rather than to build cumbersome controls to prevent problems; (b) focuses on 100% testing of transactions within selected modules, rather than sampling; and (c) is IT-intensive, rather than labor-intensive (e.g., Hermanson et al. 2006). In a continuous audit any significant discrepancies between transaction results and expected results trigger alarms that the company's operational managers, auditors, and/or top management can investigate (e.g.,

Vasarhelyi et al. 2002).[4] These alarms are automated, but the subsequent decisions regarding if and when to "drill down," or review a greater level of detail on specific items, are made by management/auditors. Only when an alarm is triggered by the system and subsequently pursued by management or an auditor does human intervention occur. The auditee will not be aware of an alarm when it is triggered by the continuous auditing system,[5] an aspect of continuous auditing that enhances its fraud deterrent effect.

How does continuous auditing affect a potential fraud perpetrator's behavior? It seems logical to believe that because of its constant, persistent presence, continuous auditing will decrease a potential fraud perpetrator's inclination to commit fraud. Continuous auditing has been touted as a powerful anti-fraud tool, as exemplified by the following quotes:

> "Continuous auditing/continuous monitoring can become a key component of an effective fraud risk management process to prevent and detect fraud and misconduct." (KPMG 2010)

> "Employee anti-fraud education that … publicizes the use of continuing audit software gives wrongdoers reasons to think twice and reduces over-reliance on internal and external audits." (Ratley 2011)

Might there be situations, however, when a continuous auditing system may actually increase fraud risk? A continuous audit is an audit by exception. If the continuous auditing system does not produce any exception reports, the underlying accounting/financial information is deemed to be free from material errors, omissions, and fraud (e.g., Chan and Vasarhelyi 2011).

---

[4] Continuous auditing techniques can be performed by management as well as auditors. Some researchers and practitioners distinguish between management-based continuous audits and auditor-based continuous audits by referring to the former as continuous monitoring and the latter as continuous auditing. See footnote 6 for additional commentary on this point.

[5] A possible exception to this would be a continuous auditing system designed to have multiple levels of alarms, in which minor or low-level alarms are brought to the attention of auditees to enhance operational efficiencies, and major or high-level alarms are made known to auditors only (e.g., Vasarhelyi and Halper 1989).

Therefore, an error, whether intentional or unintentional, that is not caught by a continuous auditing system may have the opposite of the intended effect – it may create the perception in the perpetrator's mind that s/he can easily get away with fraud. The audit-by-exception nature of continuous auditing, and the risk that all may appear fine when it actually is not, implies the need for "backup" internal audit controls of the traditional human variety. Without effective controls that catch the fraudulent acts missed by the continuous auditing system, might continuous auditing actually result in increased inclination to commit fraud on the part of a perpetrator? This is an important question that I address in my study.

The third aspect of the automated environment that I examine is whether an individual's ex ante behavior would be affected if that individual knew that feedback about her actions (including errors both intentional and unintentional) would be delivered by computer rather than by a human being. While it is true that the detection of fraudulent behavior, whether that detection is made by human audit or computerized audit, will very likely be communicated to the fraud perpetrator by a human at some point, it is entirely possible that in a computerized environment an error not yet deemed intentional, and therefore not yet deemed to be fraud, could be communicated to the person committing the error by computer rather than face-to-face human communication. Another possibility is that a fraud perpetrator could receive an initial inquiry on his actions by computer rather than directly by a human.

2.5 COMPUTERIZED AUDIT RESEARCH

Researchers in accounting and information systems (IS) have examined various aspects of computerized audits (e.g., Vasarhelyi et al. 2002; Flowerday and von Solms 2006; Hermanson et al. 2006; Kuhn and Sutton 2006; Albrecht 2008; Cook and Clements 2009; Kuhn and Sutton 2010). Most of these studies have focused on technological methods and techniques that auditors can use to enhance their audits and that firms can implement to improve their accounting and control systems. Research on computerized continuous auditing, likewise, has concentrated on technological aspects of continuous auditing. So far there has been a lack of studies on the behavioral effects of continuous auditing. Some researchers have called for experimental and empirical studies of such behavioral effects to help us understand the full impact of implementing continuous auditing systems (e.g., Hunton et al. 2004; Kuhn and Sutton 2006; Kuhn and Sutton 2010) and other types of computer monitoring (e.g., D'Arcy et al. 2009).

2.6 DETERRENCE EFFECT OF COMPUTER MONITORING

Computer monitoring is often used by organizations to gain compliance with rules and regulations, e.g., to track employees' Internet use, to record network activities, or to perform security audits (e.g., Urbaczewski and Jessup 2002). Deterrence theory suggests that computer monitoring increases perceived certainty of sanctions (e.g., Alm and McKee 2006, Wenzel 2004). Past deterrence research has shown that fear of sanctions predicts a reduction in criminal and other deviant behavior (Nagin and Pogarsky 2001). Hence, procedural and technical

countermeasures can serve as deterrent mechanisms by increasing the perceived certainty and severity of sanctions for misbehavior (e.g., Straub and Welke 1998).

Active and visible security efforts in the form of computer monitoring are recommended approaches for deterring information systems misuse based on the theoretical perspective of deterrence theory (e.g., Kankanhalli et al. 2003, Straub 1990). User awareness of security countermeasures such as computer monitoring directly impacts perceived certainty of sanctions associated with computer misuse, which in turn directly affects IS misuse intention. Like the effect of surveillance cameras described earlier, users' awareness of computer monitoring has a significant effect on users' perceived certainty of sanctions and, as a result, computer monitoring can have an enhanced deterrent effect on computer misuse (e.g., D'arcy et al. 2009).

2.7 ACCOUNTING STUDIES ON HUMAN-COMPUTER INTERACTION

Outside of the continuous auditing realm, there have been a few accounting studies that have looked into electronic versus human interaction in an accounting setting. There is mixed evidence on the issue of which is better, human or electronic interaction. Studies have looked at a variety of tasks, such as audit workpaper preparation (Brazel et al. 2004), audit workpaper review (Bible et al. 2005), and brainstorming of fraud risks (Lynch et al. 2009). Electronic audit reviews have a different effect on both reviewers and preparers than face-to-face reviews. For reviewers, electronic work environments are more cognitively demanding than traditional paper environments and impair reviewers' ability to identify errors. Auditors have been found to be

less effective in analyzing data and making decisions in an electronic environment than in a traditional paper-based environment (Bible et al. 2005).

For preparers, there is a higher sense of accountability in the face-to-face review environment than in the electronic environment. Preparers anticipating a face-to-face review are more effective and less efficient than those anticipating an electronic review (Brazel et al. 2004). The effect of an electronic environment has also been found to have a different effect on auditors' brainstorming in accordance with SAS No. 99 than a face-to-face environment. Specifically, teams that brainstorm electronically generate a greater number of relevant fraud risks than teams that brainstorm face-to-face (Lynch et al. 2009).

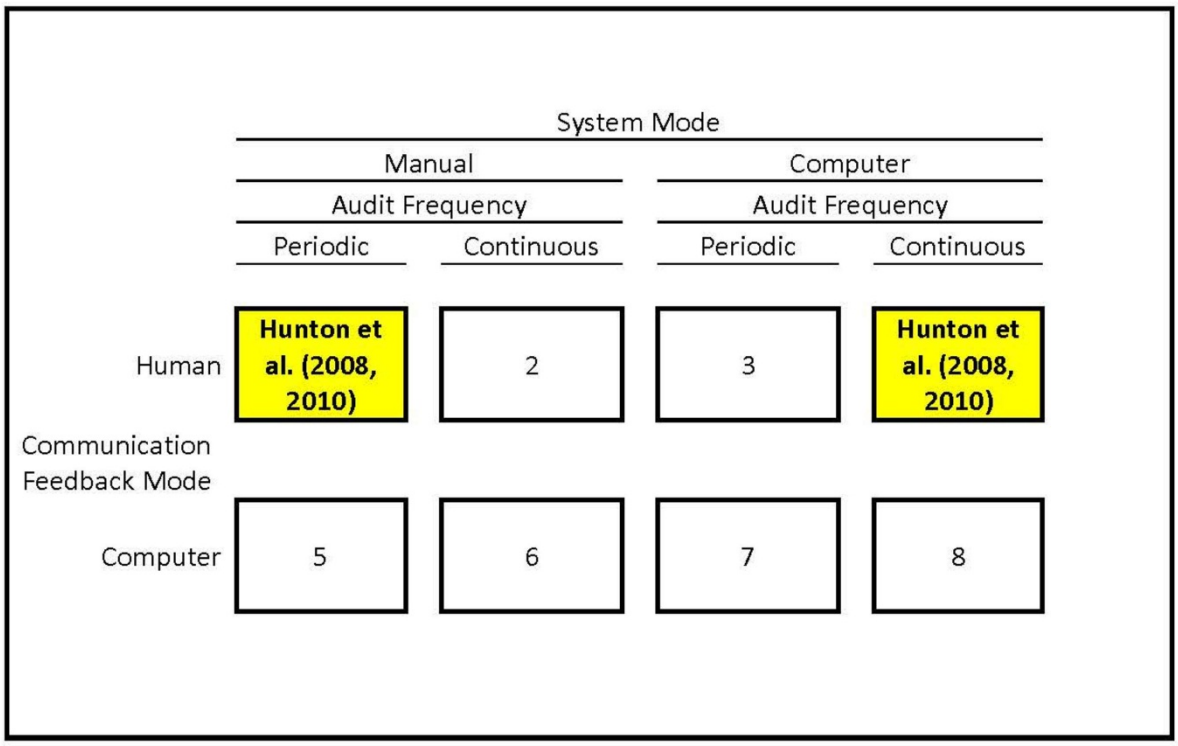
While studies such as the aforementioned have looked at differences in effects on auditors of electronic environments versus face-to-face environments, to my knowledge no accounting studies have comprehensively examined the difference in effect of these alternative environments on auditees in general or, more specifically, potential fraud perpetrators. According to the framework developed by one accounting study (Lynch and Gomaa 2003), the use of information technology in organizations can actually increase fraud risk by decreasing the frequency and intimacy of contact among people in the workplace. Decreased social contact weakens psychological ties among individuals, psychological proximity is weakened by information technology, and consequently an electronic environment increases the likelihood of a potential perpetrator attempting fraud (Lynch and Gomaa 2003).

2.8 BEHAVIORAL RESEARCH ON CONTINUOUS AUDITING

Among the few studies to date that have examined the behavioral effects of continuous auditing, two that are particularly pertinent to my study are Hunton et al. (2008) and Hunton et al. (2010). These companion studies delve into the psychological and behavioral effects of continuous auditing in a managerial decision-making context. Hunton et al.'s (2008) experiment examines how managerial decisions are affected by the interaction of monitoring frequency (periodic monitoring versus continuous monitoring) and incentive horizons (long-term versus short-term).[6] The professional manager participants in their experiment assumed the role of a manager who had to decide whether to continue a risky project and, if so, at what investment level. Hunton et al. (2008) and Hunton et al. (2010) both use an experimental design in which participants are assigned to either a periodic monitoring condition or a continuous monitoring condition. The periodic monitoring condition is presented as a traditional internal audit by human auditors, in which audits occur on a rotating but unknown (to the auditees) basis. The continuous monitoring condition is described to participants as one in which automated software collects information on a continual basis. The 2 x 2 x 2 table in Table 1 highlights the two cells examined by Hunton et al (2008, 2010).

[6] Hunton et al. (2008) distinguish continuous auditing from continuous monitoring in the following way: the former is a subset of the latter. They state that "continuous monitoring provides external auditors, internal auditors, and corporate managers the capability to track, in (near) real time, financial and nonfinancial information flowing through a company's information systems." While the term continuous monitoring can be used to refer to a process owned and performed by management, continuous auditing is a term more commonly used for an activity performed by auditors, internal or external.

Table 1 Table Highlighting Cells Examined by Hunton et al. (2008, 2010)



Hunton et al. (2008) find that, relative to periodic monitoring, continuous monitoring is more effective at decreasing earnings management of discretionary expenditures (a "functional effect") but also reduces managers' willingness to continue or otherwise increase the investment in a viable but risky project (a "dysfunctional effect"). The subsequent study, Hunton et al. (2010), sought to explain this dysfunctional risk aversion effect triggered by continuous monitoring. In Hunton et al. (2010), the authors replicate their original experiment with the exception that the professional manager-participants, rather than making the decisions themselves, evaluate the decisions of a fictitious manager. They find that, relative to periodic monitoring, continuous monitoring increases managers' perceived accountability because of managers' greater perceived need to justify their decisions under a continuous monitoring system. According to the authors, this increased accountability effect of continuous monitoring,

coupled with managers' belief that maintaining the status quo is the easiest decision to defend, explains the reduced risk-taking by managers under continuous monitoring.

Because the Hunton et al.'s (2008, 2010) studies look at two extremes (cells #1 and #4 in Table 1), they examined periodic monitoring by humans versus continuous monitoring by computers, and did not examine the intermediate conditions of periodic monitoring by a computer or continuous monitoring by a human. Because their study simultaneously varied both the audit frequency (periodic versus continuous) and the system mode (human versus computer), it did not fully disentangle the effects of these variables.[7] It is possible that, for instance, in addition to the effect of the frequency of the audit (periodic versus continuous), the system mode (computer versus human) could have driven some of their results. Additionally, participants, who volunteered for the study, assumed the role of a manager and indicated what decisions they would make regarding reporting of current expenditures and whether to continue a two-year old investment project. There was no compensation involved in the study, no consequences attached to participants' decisions, and no task repetition which might have enhanced learning. Therefore, we do not know whether Hunton et al.'s participants' perceptions would have differed if they had experienced task performance and feedback multiple times, or if their actions had a real economic effect for them.

[7] It could be argued that the timing of communication feedback in the Hunton et al. studies also varied. This argument could be made in the sense that under one condition (human/periodic) audit results are communicated to the auditee at the completion of the audit after a lapse of time while under the other condition (computer/continuous) audit results are communicated to the auditee immediately. On the other hand, an opposing argument could be made that in a continuous audit immediate feedback results do, in fact, represent feedback at the time the audit is completed, as is the case in a periodic audit. I take this latter view. I design my experiment in a similar fashion to that of the Hunton et al. studies, i.e., that audit result feedback is communicated to the auditee at the completion of the audit both in a periodic audit as well as in a continuous audit, even if in the continuous audit the communication feedback may seem to be "immediate".

3.0 THEORY AND DEVELOPMENT OF HYPOTHESES

In this chapter, I build on past research and theory to develop three pairs of hypotheses. In each case part “a” of the hypothesis predicts an effect on an individual’s perception of a condition or combination of conditions, and part “b” predicts the behavior that results from that perception.

3.1 DEVELOPMENT OF HYPOTHESIS 1

3.1.1 Perceived Certainty

Perceived certainty is a key element of perceived fraud opportunity. In criminology, deterrence theory emphasizes the important role played by a criminal’s perception of the risk of being caught, i.e., the perceived certainty of sanctions associated with performing a crime (e.g., Erickson et al. 1977; Anderson et al. 1983; Hollinger and Clark 1983). Under deterrence theory, the higher the perceived certainty, the greater the deterrence effect.

Several researchers have confirmed the importance of perceived certainty in computer users’ willingness to violate computer security (e.g., Gopal and Sanders 1997; Straub and Welke 1998; D'Arcy et al. 2009). The seminal study on employee theft (Hollinger and Clark 1983) indicates that among four independent variables – perceived certainty, perceived severity, age

and gender - by far the strongest independent variable in predicting theft is the employee's perceived certainty of being detected. Hollinger and Clark (1983) find that the employee who perceives a low certainty of theft detection is over three and one-half times more likely to steal from his employer than the employee who perceives a high certainty.

3.1.2 Computer Credibility

An important factor in the study of human-computer interaction is how individuals perceive a computer's ability to perform a task. Computers can be programmed to perform many different kinds of tasks, ranging from the simple to the highly complex: perform rote calculations; sort and summarize data input by a user; act as a decision support system, give expert advice to the user; regulate nuclear power plant operations. How well a computer is perceived to be able to perform a task is referred to as "computer credibility" (e.g., Tseng and Fogg 1999; Galletta et al. 2002; Galletta et al. 2005; Rieh and Danielson 2007).

Credibility results from evaluating multiple dimensions simultaneously, but the two dimensions that are the key components to credibility are "trustworthiness" and "expertise" (e.g., Tseng and Fogg 1999; Galletta et al. 2002). Tseng and Fogg (1999) set forth seven general categories to describe when credibility matters in human-computer interactions, one of which they call "when computers report on work performed", an example of which would be auditing. Tseng and Fogg (1999) also set forth four types of credibility: presumed; reputed; surface; and experienced. "Presumed credibility" describes how much the perceiver believes someone or something because of general assumptions in the perceiver's mind. "Reputed credibility" describes how much the perceiver believes someone or something because of what third parties

have reported. "Surface credibility" describes how much a perceiver believes someone or something based on simple inspection. "Experienced credibility" refers to how much a person believes someone or something based on first-hand experience. The first and fourth of these are pertinent to my study while the other two are not. “Reputed credibility” is not relevant to my study because the auditing system to which the participants are subject is a new one specifically created for the experiment and, hence, third parties will not have had anything to report on the system. “Surface credibility” is also not relevant: participants will not be given any prior opportunity to inspect the auditing system to which they will be subject.

3.1.3 Audit Frequency (Periodic v. Continuous Audit)

Regardless of the system mode, human or computer, a potential perpetrator’s perceived certainty of being detected will logically be related to the frequency of the audit: the more frequent the audit, ceteris paribus, the higher the perceived probability of being detected, i.e., the higher the perceived certainty. The perceived certainty of being detected in a continuous audit is higher than the perceived certainty of being detected in a periodic audit. In the field, if a potential perpetrator is monitored more often and fraud is detected earlier, he will be prevented from continuing the fraud, and as a result a continuous audit environment will result in less perceived fraud opportunity and act as more of a deterrent than a periodic audit environment. Even if the actual chance of being caught is the same, in a continuous and periodic audit environment, the prospect of getting caught earlier, and possibly more frequently, would increase the perpetrator’s perceived certainty of his fraudulent act being detected in a continuous auditing environment.

While a continuous audit environment may act as a successful deterrent against some potential fraud perpetrators some of the time, the possibility remains that not all potential fraud perpetrators will be fully dissuaded all of the time. As previously described, experienced credibility emanates from a person having first-hand experience with a computer (Tseng and Fogg 1999). An effective continuous auditing system, i.e., one with a high detection probability, will likely result in high experienced credibility in the mind of the potential fraud perpetrator. Conversely, an ineffective continuous auditing system, i.e., one with a low detection probability, will likely have the opposite effect. If a fraud perpetrator attempts a fraudulent act and, because of a low probability of detection, the continuous audit environment does not detect the fraud, it is likely that the perpetrator will perceive a reduced probability of getting caught. This is analogous to tax audit environments where, because there is a low probability of being audited, successful tax evaders update their perceptions of being detected, and evade taxes more in the future (e.g., Snow and Warren 2007). I predict that audit frequency and actual detection probability will interact and influence, as explained below, both fraud perpetrators' perceptions about the likelihood of being detected (i.e., their perceived opportunity to commit fraud) and their propensity to commit fraud. Specifically, continuous auditing's relative effectiveness will depend on the actual probability of fraud detection, as described in the hypotheses that follow. I make separate predictions regarding the effects on participants' perceptions and their actions. I formally state my first pair of hypotheses next, and illustrate them in Figure 1:

> **H1a**: The effect of Audit Frequency on Perceived Opportunity will depend on the Actual Detection Probability. These two factors will interact such that when there is a high actual probability of fraud detection, a continuous audit environment will create a lower perceived opportunity to commit fraud than a periodic audit environment. However, when there is a low actual probability of fraud detection, a continuous audit environment will create a higher perceived opportunity to commit fraud than a periodic audit environment.

H1b: The effect of Audit Frequency on Fraud Percentage will depend on the Actual Detection Probability. These two factors will interact such that when there is a high actual probability of fraud detection, a continuous audit will be more effective at deterring fraud and result in a lower percentage of fraudulent behavior than a periodic audit. However, when there is a low probability of fraud detection, a continuous audit will be less effective at deterring fraud than a periodic audit and will result in a higher percentage of fraudulent behavior.

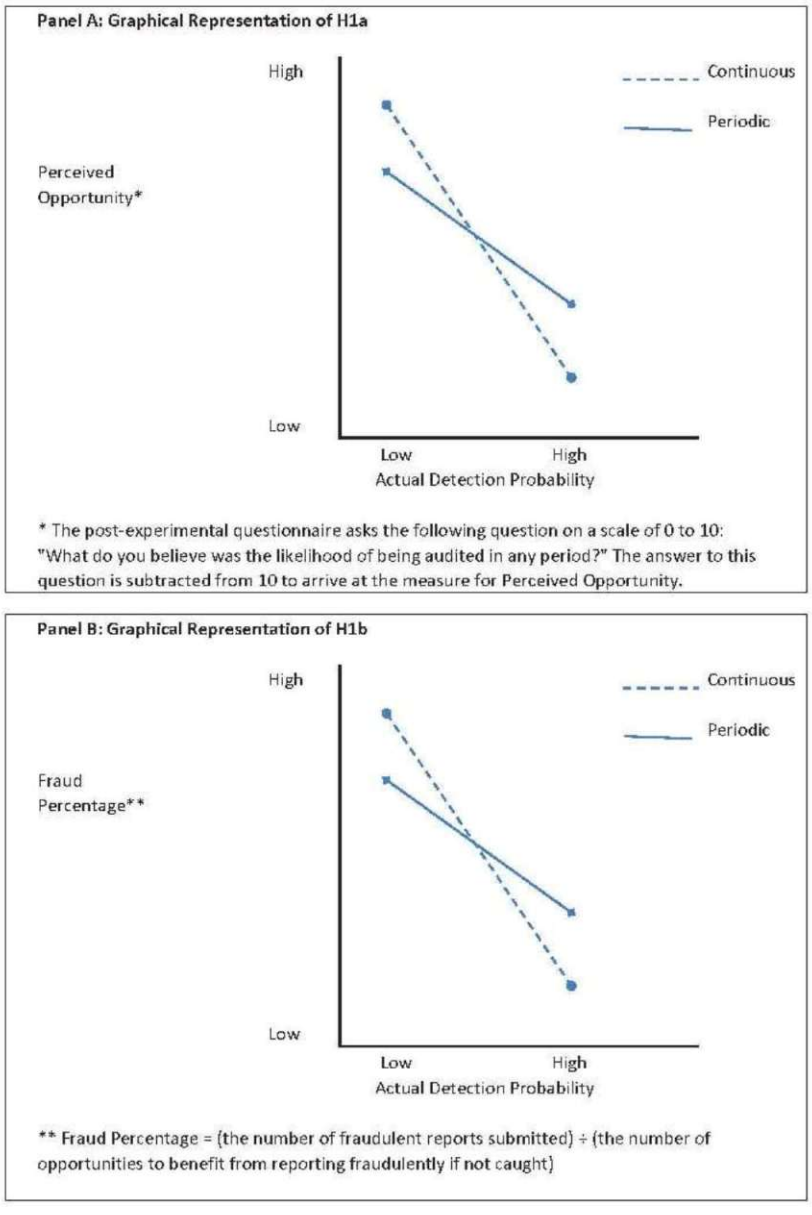


Figure 1 Hypothesized Interaction Effects for Experiment 1

3.2 DEVELOPMENT OF HYPOTHESIS 2

3.2.1 Credibility in Human-Computer Interaction

Several researchers have demonstrated that computers are generally assigned more credibility than humans. Computers have a scientific mystique, considered to be wholly objective and superior to humans in performing tasks. Computers are seen as powerful and sometimes intimidating machines, with superior wisdom to humans in a way that makes them seem faultless (e.g., Sheridan et al. 1983). Computers are "awesome thinking machines" (Pancer et al. 1992). People believe that expert advice given by a computer is more objective and rational than that given by human advisers (e.g., Dijkstra et al. 1998). Under the Tseng and Fogg (1999) model described earlier, a computer derives high computer credibility from a high *presumed* credibility. People think humans make mistakes and consequently human error is considered a very significant problem for organizations (e.g., Deloitte 2007). Extending this to audit detection, I expect that people perceive higher credibility in computerized audits than in human audits.

Thus, if potential fraud perpetrators perceive higher credibility in computerized audits than in human audits, the higher credibility assigned to computerized audits contributes to those individuals' perceived certainty of being detected. Although the actual probability of detection may be identical between two types of audits, computerized and human, the perceived certainty of being detected will nevertheless be higher for the computerized audit. In turn, based on deterrence theory as previously described, potential fraud perpetrators' higher perceived certainty of detection by a computerized audit will result in the computerized audit serving as a greater deterrent than a human audit, *ceteris paribus*. Therefore, fraud perpetrators will be less

willing to attempt fraud in a computerized system environment in which audits are computerized than in a manual system environment in which audits are performed by humans.

While many researchers maintain that people perceive computers to be highly credible, some researchers have argued otherwise. They take the alternate view that, while people have generally held computers in high regard since the inception of their usage, the credibility of at least some computers has declined over time. The argument is that, like many aspects of our human society, computers are facing a credibility crisis (e.g., Rieh and Danielson 2007; Tseng and Fogg 1999), due in part to the popularization of the Internet, the ease with which false information may be disseminated through the Internet, and the fact that many people have become skeptical of what they read on the Internet. Tseng and Fogg (1999, p. 39) note that "If the pendulum swings too far in this direction, computers--especially with respect to Web-based content--could be viewed as among the least credible information sources, rivaling TV infomercials and supermarket tabloids for such dubious distinction."

3.2.2 System Mode (Human v. Computerized)

The studies that find that people perceive computers to be more credible than humans seem to be those that examine more objective tasks like computerized word processing (Pancer et al. 1992), problem solving by computerized expert systems (Dijkstra et al. 1998), and others such as aircraft control systems (Sheridan et al. 1983). In contrast, the studies that find computers to be less credible appear to be set in more subjective contexts like computers being given the task of making semi- to fully-subjective judgments (e.g., Honaker et al. 1986; Andrews and Gutkin 1991; Lerch 1997) or human-created Web-based information (Tseng and Fogg 1999). Because

the setting in this study (i.e., a computerized audit task) is objective in nature it is likely that a potential fraud perpetrator will perceive a computer to be more skillful than a human at performing the task of auditing. Therefore, I predict that the computerized audit in a computerized system will increase perpetrators' perceived certainty of being detected (i.e., it will reduce their perceived opportunity to commit fraud) as well as their actual fraudulent behavior. This prediction leads to the following pair of hypotheses about participants' perceptions and actions, respectively:

> **H2a**: When the actual detection probability is held constant, potential fraud perpetrators will have a lower perceived opportunity to commit fraud when audits are performed by a computer in a computerized audit system than when they are performed by a human in a manual system.
>
> **H2b**: When the actual detection probability is held constant, computerized audits in a computerized system will be more effective at deterring fraud and result in a lower percentage of fraudulent behavior than will be audits performed by humans in a manual audit system.

3.3 DEVELOPMENT OF HYPOTHESIS 3

3.3.1 Computer-Mediated Communication

As previously described, an individual's perceptions regarding human-computer interaction could be influenced by whether a computer performs a given task, e.g., an audit. Another way that an individual's perceptions could be influenced is through computer-mediated communication, such as e-mail.

Computer-mediated communication differs from direct types of human interaction in several important ways. Computer-mediated communication does not have the aural or visual feedback of face-to-face communication. In face-to-face communication, nonverbal behavior such as head nods, smiles, eye contact, physical distance, and tone of voice, give speakers and listeners information they can use to regulate, modify, and control exchanges. In computer-mediated communication there is no opportunity to hear the other's voice or to look her in the eye (e.g., Kiesler et al. 1984). Additionally, e-mail and other computer-mediated communication, being asynchronous, allow people time to reflect before responding. This gives a potential liar, or perhaps a potential fraud perpetrator, time to think about how to best conceal his deception. On the other hand, synchronous communication, e.g., face-to-face communication, does not allow a liar the luxury of time to formulate lies (e.g., Whitty and Carville 2008). Individuals may feel more confident that they will get away with lying, or other dishonest behavior, in a computer-mediated communication environment, in which they have time to think about and weave their deception. As discussed earlier, Lynch and Gomaa's (2003) study suggests that a computerized work environment increases the likelihood that employees will attempt fraud.

3.3.2 Lying in Computer-Mediated Communication

There are four potential theories that would predict that individuals lie more, and otherwise behave more dishonestly, in computer-mediated communication than in direct human interaction: social distance theory, moral disengagement theory, deindividuation, and social identity theory. Social distance theory holds that social distance between people varies depending on the media, and that this distance predicts the extent to which people are willing to

behave dishonestly under different communication media. For example, social distance theory predicts that because there is greater space between people when they communicate by telephone than when they engage in face-to-face communication, more people will lie on the telephone than when meeting in person. The theory's reasoning is based on the fact that lies are likely to make the liar feel uncomfortable and apprehensive (DePaulo and Kashy 1998; Whitty and Carville 2008), and that social distance serves to lessen the liar's discomfort and apprehension. Therefore, computer-mediated communication (e.g., e-mail) provides greater space between individuals than does telephone, which provides greater space than face-to-face interaction. Accordingly, social distance theory holds that, all else equal, it is easier for a person to lie in computer-mediated communication such as e-mail than in face-to-face conversation. This theory has been confirmed in studies such as one that showed that individuals lie proportionately more on the telephone than in face-to-face communication (Whitty and Carville 2008).

Related to social distance theory is moral disengagement theory, which asserts that one can maintain a set of internal moral standards yet still behave in ways inconsistent with those standards in some situations. According to this theory, people release themselves from guilt and responsibility for deviations from a self-regulatory moral code through several mechanisms, among which are finding psychological ways to distance themselves from the harmful consequences of their actions (Bandura 1999). Hence, individuals contemplating a dishonest act, such as fraud, that runs counter to their moral standards would likely feel greater social distance between themselves and those who would be harmed by their act, and less guilt in performing the dishonest act, when interacting via computer than when interacting in person with another individual.

In deindividuation, reduced attention to self and others elicits behavior that is relatively unrestrained and unregulated. Kiesler et al. (1984) note that computer-mediated communication has many of the factors that contribute to deindividuation, including reduced self-regulation and reduced self-awareness, and weakens social influence that is otherwise present in face-to-face interaction. Computer-mediated communication, in comparison to face-to-face communication, reduces feelings of embarrassment, guilt, and empathy for others; produces less social comparison with others; and reduces fears of retribution or rejection. Use of the computer itself has an effect on behavior. The act of using the computer tends to be absorbing and conducive to quick response, which reduces self-awareness and increases the feeling of being submerged in the machine. Thus, computer-mediated communication induces an overall weakening of self-regulation similar to what happens when people become less self-aware and submerged in a group (e.g., Kiesler et al. 1984).

According to social identity theory, people identify with and cooperate with people like themselves. It is useful for predicting behavior in a computerized environment where people may be less willing to cooperate with a computer than with another person because they view a computer as being less like themselves. In an experimental study in which participants faced a prisoner's dilemma situation with either a human partner or a computer partner with varying humanlike attributes, individuals who played the prisoner's dilemma game with a partner represented as a computer cooperated less than when they played the game with an actual person (Kiesler et al. 1996).

3.3.3 Communication Feedback Mode (Human v. Computer Feedback)

For purposes of this study, it is not important to distinguish among the four theories described above. Rather, what is important is that all four would make the same prediction: individuals lie more, and otherwise behave more dishonestly, in computer-mediated communication than in direct human interaction.

An opposing view regarding the extent to which people are willing to lie in computer-mediated communication is that held by media richness theory (e.g., Hancock et al. 2004), sometimes referred to as information richness theory. Media richness theory maintains that rich media, such as face-to-face communication, has multiple cue systems, immediate feedback, natural language and message personalization, and provides users with more equivocal communication activities According to this view, lying can be considered highly equivocal. When weaving a deceptive story, rich media provides more avenues for the liar to utilize. Face-to-face communication provides the liar flexibility in ways to respond that would not be available in e-mail or other computer-mediated communication.

However, while media richness theory would predict that users would lie more often in a face-to-face environment than in a computerized environment, it does not seem to match my setting. Media richness would be more descriptive in cases where the fraudster could weave a "full story" and use a variety of media to convince the targeted party of the veracity of his lie, and could serve as a good predictor of behavior under such elaborate-story situations. In the current setting, where the fraudster is attempting to hide a straight fact, rather than weave an elaborate story, the other four theories described earlier are much more applicable.

The four theories described in section 3.3.2 would predict that potential fraud perpetrators will be more inclined to attempt fraud when they expect feedback through computer-mediated communication than when they expect face-to-face feedback from a human. This arises, not because of a difference in perpetrators' perceived probability of detection between the alternative communication feedback systems, but because of a difference in perpetrators' sense of comfort

between having to explain their actions through computer-mediated communication and in a face-to-face conversation with a human. My final pair of hypotheses is formally stated as:

> **H3a**: A potential fraud perpetrator will feel more uncomfortable receiving feedback about having attempted to commit a fraud if that feedback is communicated face-to-face by a human than if the feedback is communicated via computer.
>
> **H3b**: When feedback regarding a user's attempted or actual fraud is communicated by computer, potential fraud perpetrators will be more willing to attempt fraud than when feedback is communicated in face-to-face communication. Therefore, the human feedback mode will more effectively deter fraud and result in a lower percentage of fraudulent behavior than will the computer feedback mode.

4.0 METHOD

4.1 OVERVIEW

This study is composed of two experiments. Experiment 1 tests the effects of continuous versus periodic auditing, predicted in hypothesis 1 (H1a and H1b). Experiment 2 tests the effects of the computerized versus manual system mode, predicted in hypothesis 2 (H2a and H2b), and the effects of the human versus computer communication feedback mode, predicted in hypothesis 3 (H3a and H3b). In the remainder of this chapter I describe the two experiments)[8].

4.2 EXPERIMENT 1

4.2.1 Participants

Participants for my experiments were recruited through the Pittsburgh Experimental Economics Laboratory pool, which is primarily composed of University of Pittsburgh undergraduate and graduate students from a variety of fields of study (e.g., business, economics, humanities,

[8] Both experiments were conducted with the approval of University of Pittsburgh's Institutional Review Board (IRB).

psychology) as well as a few Carnegie Mellon University full-time students and a few non-student working individuals. The average age range of participants in Experiment 1 was 20 to 29 years old. I conducted several 90-minute experimental sessions, each of which consisted of 20 periods[9], to obtain 24 participants in each of four experimental conditions, for a total of 96 participants. During an experimental session participants interacted only with the auditor; there was no interaction among participants. The ratio of male to female in Experiment 1 was 54:42.[10]

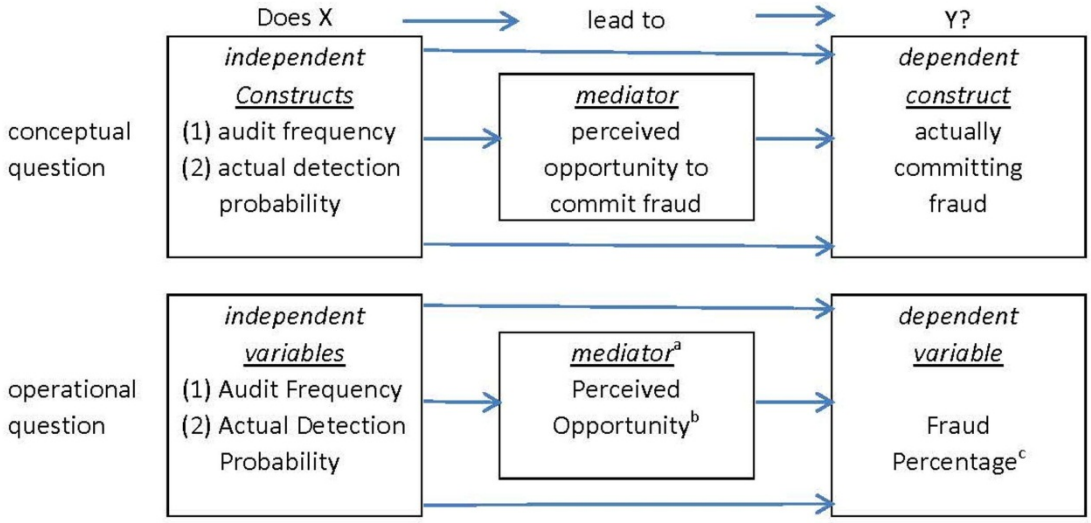
4.2.2 Design: Audit Frequency

Experiment 1 is a 2 x 2 between-subjects design. It is designed to test H1a and H1b by varying the independent variables Audit Frequency (Periodic, Continuous) and Actual Detection Probability (Low=15%, High=85%).[11] Figure 2 portrays the conceptual constructs and corresponding operational variables, and Panel A of Table 2 illustrates the experimental design matrix and the cells tested in Experiment 1.

[9] To avoid creating conditions that would be conducive to end-of-game behavior, participants were not informed of the planned number of periods beforehand.

[10] Post-experimental statistical analyses showed no significant differences across gender.

[11] In pilot study testing I manipulate Actual Detection Probability at three levels (Low=15%, Medium=50% and High=85%) and find that the results for the Medium condition are similar to those for the High condition. Accordingly I eliminated the Medium condition in subsequent experimental sessions and used only the High and Low levels of Actual Detection Probability.



[a]Mediator variable is both an independent variable and a dependent variable. It is hypothesized that the dependent variable in H1a, Perceived Opportunity, mediates the effect on the other dependent variable, Fraud Percentage, in H1b.

[b] Perceived Opportunity is measured using participants' answers to the post-experimental question on perceived probability of detection: "What do you believe was the likelihood of being audited in any period?" Answers on an 11-point scale range from "no chance of being audited" (0 on the scale) to "very high likelihood of being audited" (10 on the scale). Because perceived opportunity to commit fraud is inversely related to the perceived probability of detection, I calculate Perceived Opportunity by subtracting the perceived probability of detection from 10.

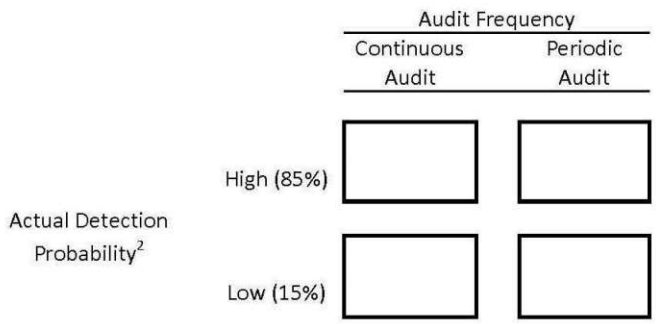
[c] Fraud Percentage = (the number of fraudulent reports submitted) ÷ (the number of opportunities to benefit from reporting fraudulently if not caught).

Figure 2 Experimental Design for Experiment 1 (H1a and H1b)

[*]Also see Table 2, Panel A which shows an experimental design matrix that summarizes the operationalization of the cells that are tested in Experiment 1.

Table 2 Designs for Experiment 1 and Experiment 2

Panel A: Experiment 1 Design (H1a and H1b)[1]



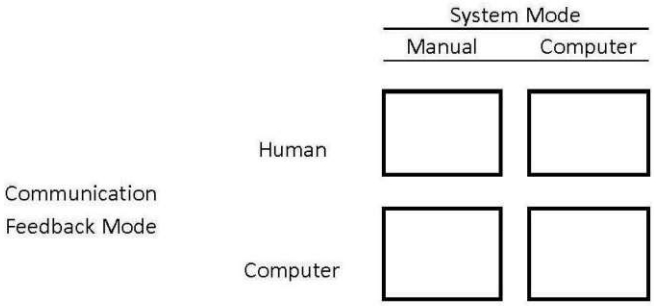
Dependent Variables:

- H1a: Perceived Opportunity; H1b: Fraud Percentage

[1] All audits in Experiment 1 use Computerized System Mode and Computer Communication Feedback Mode.

[2] In a pilot study I manipulated Actual Detection Probability at Low, Medium and High and find that Medium is similar to High. I thus eliminate the Medium level in the experiments.

Panel B: Experiment 2 Design (H2a, H2b, H3a, H3b)[3]



Dependent Variables:

- H2a: Perceived Opportunity; H2b: Fraud Percentage
- H3a: Feeling When Caught; H3b: Fraud Percentage

[3] All audits in Experiment 2 use Continuous Audits and Low Actual Detection Probability.

The dependent variable to test H1a is Perceived Opportunity, and is measured by using participants' answers to the post-experimental, eleven-point scale question "What do you believe was the likelihood of being audited in any period?" Answers on an 11-point scale range from "no

chance of being audited" (0 on the scale) to "very high likelihood of being audited" (10 on the scale). Because Perceived Opportunity to commit fraud is inversely related to the perceived chance of detection measured by the question, the dependent variable Perceived Opportunity is calculated by subtracting the participant's answer regarding the likelihood of being audited from the highest point on the scale, "10." For example, if the participant chose "3" as the perceived chance of detection, then Perceived Opportunity was calculated as 10 minus 3, or 7. The dependent variable to test H1b is Fraud Percentage, and is calculated by dividing the number of fraudulent reports submitted by the number of fraudulent reporting opportunities.

The two levels of Audit Frequency, Periodic Audit and Continuous Audit, differ in the timing of the audit. The difference is that in a Continuous Audit an audit occurs each period, immediately after the performance of the task, whereas in a Periodic Audit an audit occurs after several periods have passed. Panel A of Table 3 illustrates the timing of the audit under each type of audit. Assume that the experiment has twenty periods and that, as a result of random selection based on the Actual Detection Probability, periods 3, 7, 14 and 17 are selected for audit. Further, assume that under the Periodic Audit condition two audits occur, an interim audit at the end of the twelfth period and a second audit at the end of the twentieth period. In other words, in a Continuous Audit, the audit for a selected period is performed immediately upon the task being completed for that period, prior to the start of the subsequent period, whereas in the Periodic Audit condition the periods selected for audit are all audited at the same time.

Table 3 Examples, Description of Experiments

Panel A: Example of Timing of Audits

Period	selected for audit?	timing of audit under: continuous audit	timing of audit under: periodic audit
P1	no	-	P3 and P7 audited at end of P12
P2	no	-	
P3	YES	at end of P3	
P4	no	-	
P5	no	-	
P6	no	-	
P7	YES	at end of P7	
P8	no	-	
P9	no	-	
P10	no	-	
P11	no	-	
P12	no	-	
P13	no	-	P14 and P17 audited at end of P20
P14	YES	at end of P14	
P15	no	-	
P16	no	-	
P17	no	at end of P17	
P18	no	-	
P19	no	-	
P20	no	-	

Table 3 (continued)

Panel B: Example Table of Data Collected

A	B	C	D	E	F	G	H	I	J
			Total		Participant's				
		Item	Amount	Item	Share	Reported	Audited	Penalty,	Net
Period	Mgr #	Collected	Collected	Reported	Received	Honestly?	or Not?	if any	Earnings
1	1	A	$21.60	A	$0.60	YES	AUDIT	$0.00	$0.60
2	1	B	$21.60	B	$5.40	YES	NOT	$0.00	$5.40
3	1	A	$21.60	A	$0.60	YES	AUDIT	$0.00	$0.60
4	1	B	$21.60	B	$5.40	YES	NOT	$0.00	$5.40
5	1	B	$21.60	B	$5.40	YES	AUDIT	$0.00	$5.40
6	1	A	$21.60	B	$5.40	NO	NOT	$0.00	$5.40
7	1	A	$21.60	B	$5.40	NO	AUDIT	($7.20)	($1.80)
8	1	B	$21.60	B	$5.40	YES	NOT	$0.00	$5.40
9	1	A	$21.60	B	$5.40	NO	AUDIT	($7.20)	($1.80)
10	1	A	$21.60	B	$5.40	NO	NOT	$0.00	$5.40
11	1	A	$21.60	A	$0.60	YES	AUDIT	$0.00	$0.60
12	1	B	$21.60	B	$5.40	YES	NOT	$0.00	$5.40
13	1	B	$21.60	B	$5.40	YES	AUDIT	$0.00	$5.40
14	1	A	$21.60	B	$5.40	NO	NOT	$0.00	$5.40
15	1	A	$21.60	B	$5.40	NO	AUDIT	($7.20)	($1.80)
16	1	A	$21.60	A	$0.60	YES	AUDIT	$0.00	$0.60
17	1	B	$21.60	B	$5.40	YES	NOT	$0.00	$5.40
18	1	B	$21.60	B	$5.40	YES	NOT	$0.00	$5.40
19	1	A	$21.60	B	$5.40	NO	AUDIT	($7.20)	($1.80)
20	1	A	$21.60	B	$5.40	NO	NOT	$0.00	$5.40

Actual Detection Probability is the actual probability of being selected for audit in any one period. Recall that H1a and H1b predict it would interact with Audit Frequency as illustrated in Figure 1. I manipulate Actual Detection Probability at Low (15%) and High (85%) in the experiment as an abstraction of a real world audit environment with design weaknesses that can be exploited by a fraud scheme that would not always be discovered. For example, although continuous auditing in practice is designed to test 100% of transactions, a fraud perpetrator could create a fraud scheme that has not yet been anticipated by auditors. That is, a big concern in companies is that auditors may not have built tests into the continuous auditing system to detect

all possible fraud schemes. Hence, depending on the perpetrator's fraud scheme and the design of the continuous auditing system, the effective detection probability is likely to be less than 100%, and could even approach 0%.

4.2.2.1 Task

My design conforms to the well-established custom in experimental economics type research of having participants perform a relatively simple task repeatedly in multiple periods (see, for example, Kagel and Roth 1995 and Loewenstein 1999). Participants in my experiment perform the same specific task, that of submitting a collections report as described shortly, in multiple periods. All task performance is auditable (i.e., each period can be selected for audit).

Participants assume the role of a company manager who makes collections, retains a portion of those collections, and submits collection reports. In each period of an experimental session, participants prepare and submit reports about which of two items, Item A or Item B, they collect for the period. While the amount collected is identical for Items A and B, the amount participants retain for each of the two items differs, i.e., they retain more when they collect Item B than they do when they collect Item A. Participants' compensation is based on the reports they submit for each period, adjusted for the results of any audits.

At the beginning of each period participants are informed by computer which item they actually collected in that period. They then prepare and submit via computer an electronic Report Form for the period indicating which item they collected. Audits are performed by a computerized audit program, i.e., an automated computerized auditor performs an audit of an electronic Report Form submitted by the participant. Participants do not know in advance which period(s) will be audited, and they are informed of audit results via computer.

In some periods, exogenously determined on a random basis and unknown to participants beforehand, participants can report opportunistically, i.e., report fraudulently, and, as a result, can potentially receive higher compensation than they would by reporting honestly. Such opportunities arise when a participant is informed that s/he collected Item A, the lower-paying item. However, this opportunity also carries risk of detection if a period in which the participant reports fraudulently is randomly selected for audit. If fraudulent behavior is uncovered by the audit, the participant pays a monetary penalty that results in a net loss for the period. The experiment is designed such that all audits are 100% successful, i.e., the audit of any period in which a participant reports fraudulently always reveals the fraud[12]. Periods are randomly selected for audit and the probability of being audited is a manipulated variable, as explained shortly. Participants are informed of the compensation structure and the payoffs associated with reporting honestly versus reporting fraudulently, but are not informed of the probability of a period being audited[13].

Participants can report honestly or dishonestly. For purposes of this study, a false report is deemed a fraudulent act, as it represents an intentionally dishonest act for the purpose of financial gain. This is very similar to what occurs in actual frauds that occur in the workplace, referred to as occupational fraud which is defined as:

---

[12] This is an abstraction from the real world in which audits are not necessarily 100% effective in uncovering fraud when it occurs. In both the real world and in this study the probability of being detected is a combination of the probability of being audited and the probability of the audit successfully detecting fraud, i.e., Prob(detection) = Prob(audit) x Prob(auditor detecting fraud). In my study I assumed the latter probability is 100%, such that Prob(detection) = Prob(audit) x Prob(auditor detecting fraud) = Prob(audit) x 100% = Prob(audit). Hence, in this study audits are exogenously determined at random and unknown to participants before the fact, and are 100% effective. This slight abstraction from the real world allows me to maintain simplicity and control without compromising the strength of the experiment to answer the research questions.

[13] In pilot study testing I manipulate the level of information about Actual Detection Probability that I provided to participants at three levels (Actual Probability, Actual Range, No Probability Provided). In my main experiments this level is held constant at No Probability Provided, i.e., participants are not provided with information on the actual detection probability.

"the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (ACFE 2012).

Although this study's experimental setting represents an actual fraud setting in which the perpetrator engages in an intentionally deceptive act for his or her own personal gain, no direct or indirect references to fraud are made during the experiment. Moreover, participants are not encouraged to submit either honest or dishonest reports.

Appendices A through E present the experimental procedures and related forms, including details of the experimental task.

4.2.2.2 Parameters

My experiment incorporates economic incentives designed to elicit "true economic" behavior from the participants (see, for example: Kagel and Roth 1995; Loewenstein 1999). The key economic parameters in the experiment are the following: (1) fixed initial endowment; (2) the monetary payoff for reporting each item type, A and B; (3) the penalty paid for reporting fraudulently and being caught by the auditor; (4) the actual probabilities of collecting items A and B, respectively; (5) the probability of being caught reporting fraudulently, which is equal to the probability of being audited, and (6) the number of periods. In all conditions of both experiments participants are told about the first four of these items, but are not provided information about the actual detection probability or the planned number of periods.[14]

The values for the economic parameters of my study are as follows:

- Fixed initial endowment = $5.00

[14] In pilot testing I manipulate the level of information about Actual Detection Probability provided to participants, varying it so that in some conditions participants receive some information, which is explained in subsection 5.1 Pilot Study, but in the full experiments no information about Actual Detection Probability is provided to participants.

- Amount retained by participant for reporting the collection of Item A = $0.60
- Amount retained by participant for reporting the collection of Item B = $5.40
- Penalty for being caught reporting fraudulently[15] = $7.20
- Probability of collecting Item A = 60%
- Probability of collecting Item B = 40%
- Probability of being caught reporting fraudulently = Probability of being audited. In Experiment 1, this was manipulated at 15% and 85%.

I set the above parameters to create conditions in which participants could expect a reasonable, but unknown, compensation (in the $10 to $25 range) based in part on the choices they made between the less risky option (reporting honestly) and the riskier option (reporting fraudulently). See Table 4 for participants' expected values when they are 100% honest versus when they are 100% dishonest under alternative Actual Detection Probability levels.

[15] A participant would report fraudulently if he collected Item A but reported Item B, thereby retaining the higher amount between the two items. A participant would not have any opportunity to commit fraud, i.e., report fraudulently, if he collected Item B since he would already be receiving the maximum amount between the two items by reporting honestly. For purposes of calculating expected values I assume that in all cases when Item B is collected the participant reports the collection of Item B, because in such case the honest report represents the higher outcome.

Table 4 Participant Expected Values

	Actual Detection Probability L (15%)	H (85%)
expected value - 100% honesty[1]	$17.60	$17.60
expected value - 100% dishonesty[2]	$28.85	$14.15

notes:

[1] *see calculation below, for item K*

[2] *see calculation below, for item L*

Prob(Item A, the lower paying item)	A	60%	60%
Prob(Item B, the higher paying item)	B	40%	40%
Proceeds(Item A reported)	C	$0.60	$0.60
Proceeds(Item B reported)	D	$5.40	$5.40
Penalty(Item B reported & audited)	E	($7.00)	($7.00)
Prob(being audited)	F	15%	85%
Fixed endowment	G	$5.00	$5.00
Number of periods	H	5	5
ExpVal(100% honesty) =			
[[(A x C) + (B x D)] x H)	I	$12.60	$12.60
ExpVal(100% dishonesty) =			
([A x [((1 - F) x D) + (F x (D + E))] +			
(B x D)] x H)	J	$23.85	$9.15
ExpVal(100% honesty) + fixed			
endowment = I + G	K	$17.60	$17.60
ExpVal(100% dishonesty) + fixed			
endowment = J + G	L	$28.85	$14.15
Ratio of L to K	M	1.64	0.80

To illustrate, I refer to Panel B of Table 3 which provides an example table of data collected for a hypothetical participant ("Manager # 1") for the first twenty periods of an experimental session. The column labeled "C" shows the item collected, A or B, that was randomly assigned to the participant, and column D shows the corresponding amount collected, an amount that is the same for items A and B. The next column, E, shows which item, A or B,

the participant reports as collected and column F reflects the corresponding participant's share received, i.e., how much of the amount in column D the participant would keep based on the item reported in column E. Columns G and H indicate whether the participant reports honestly and whether s/he is audited, respectively. The last two columns, I and J, show the penalty, if any, and net earnings for the period, respectively. Participants are given a fixed endowment of $5.00 at the start of the experiment, to ensure that no participants face a negative cash balance during the experiment, which could distort their decision-making.

I assume participants are risk averse to the same extent as has been found in previous experimental studies that measured risk aversion (e.g., Holt and Laury 2002; Harrison et al. 2005; Colombier et al. 2008). Because fraudulently reporting is a riskier option than is reporting honestly, I built a risk premium into the compensation structure to increase the attractiveness of the riskier option relative to the less risky option. I also include Holt and Laury's (2002) risk measurement questions in my post-experimental questionnaire (see the set of questions in the last part of Appendix E) to confirm participants' level of risk aversion.

Table 4 presents the expected values of always reporting honestly versus always reporting dishonestly when there's an incentive to do so, given the actual detection probabilities (low and high), and the payoffs under the compensation structure used in my experiments. As shown in the table, in the Low 15% Actual Detection Probability condition there is a considerably higher payoff for always reporting dishonestly than for always reporting honestly; in the High 85% Actual Detection Probability condition there is a modestly lower payoff for always reporting dishonestly than always reporting honestly. Although participants are not informed of the actual detection probability, as the experiment progresses and they receive feedback they are able to make inferences about that probability. Hence, ceteris paribus, one can

expect higher fraudulent behavior in the Low 15% condition than in the High 85% condition (which proved to be the case as reported later). Importantly, my hypotheses do not relate to this main effect of low detection probability being less of a fraud deterrent than high detection probability. Rather, H1a and H1b predict a differential effect of the continuous versus periodic audit approach in each of these actual detection probability conditions (i.e., H1a and H1b predicts an interaction, not a main effect).

4.2.2.3 Random Lottery Incentive Mechanism

Participants in each experimental session perform their assigned task repeatedly over multiple periods. There are three possible monetary outcomes for a participant in any given period: (1) earnings resulting from reporting the low paying item (Item A); (2) earnings resulting from reporting the high paying item (Item B); and (3) net negative earnings resulting from fraudulently reporting the high paying item (Item B) and being detected by the audit system.

An issue that arises in economics type experiments such as this one is how to structure the incentives so that participants' behavior is not distorted. If, for example, participant compensation was structured such that the total of all periods' earnings was paid at the end of the experimental session, and participants had knowledge of this from inception, this could influence participants' behavior. Participants' behavior under such a cumulative incentive structure could potentially be distorted by one or more effects, such as wealth effects, portfolio effects, income effects and house money effects (see, for example: Charness and Kuhn 2010; Cox et al. 2011; Nelson 1998). The essence of all of these types of effects is that participants' knowledge that they are accumulating wealth as the experiment progresses may affect their decision-making. The widely accepted practice among experimental economists to address these issues is to pay

for some random subset of all periods, rather than paying for all periods, at the end of the experiment. This payment mechanism is known as the random lottery incentive mechanism (e.g., Charness and Kuhn 2010; Hey and Lee 2005).

Randomly selecting one period for payment provides simplicity and, given a pre-determined budget, allows the experimenter to offer participants a higher per-period payout than selecting multiple periods for payment. Some experimentalists believe that higher payout amounts enhance the perception among participants of real work for real money (e.g., Charness and Kuhn 2010).

Randomly selecting more than one period for payment is considered to have the same effect as selecting one period for payment (e.g., Charness and Kuhn 2010).[16] My informal discussions with several experimental economists confirmed agreement on this point.[17] Depending on circumstances, it may make good sense to randomly select more than one period for payment. For example, Bracha et al. (2011) randomly select three out of 14 periods for payment.

I determined that for my study the random selection of more than one period for payment would be more appropriate than the random selection of only one period, for two reasons. First, randomly selecting multiple periods reduces the likelihood of a participant being paid less than the initial endowment. For example, in a one-period pay system, the single period selected for payment could be a period in which a participant fraudulently reports and is detected, and the

[16] The effect is considered the same only if the number of periods selected is a sufficiently small percentage of the total number of periods. If the number of periods selected for payment is high compared to the total number of periods in the experiment, then the effects previously mentioned (wealth effect, etc.) would once again be an issue. The experimenter's decision of how many periods would be "too many" is subjective.

[17] I held informal discussions on this point with experimental economists on the faculty of University of Pittsburgh and two other universities, as well several current or former doctoral economics students at the University of Pittsburgh.

participant would therefore end the experiment with negative earnings. The second reason relates to the large variance among the three possible monetary outcomes for a participant in any given period (described above). The three possible outcomes represent monetary factors of x, 9x and -12x, respectively. If only one period is selected for payment, a participant faces the risk that this period is not representative of all his/her behavior and could be an extreme negative outcome (i.e., -12x). It is possible that a participant's perception of this risk could dominate his/her behavior during the experiment, and overpower the effects of the other variables of interest. Therefore, to alleviate these concerns, I pay participants for five randomly selected periods.

4.3 EXPERIMENT 2

4.3.1 Participants

Participants for Experiment 2 were also recruited through the Pittsburgh Experimental Economics Laboratory pool, and were similar to those in Experiment 1. In Experiment 2, there were 24 participants in each cell, for a total of 96 participants. It should be noted that this represents 72 new participants (three cells of 24 participants each) and 24 participants who were used in one of the cells in Experiment 1.[18] During an experimental session participants interacted with either a human auditor or a computerized auditor (depending on the session), and there was

[18] The Low 15% Audit Detection Probability / Continuous Audit Frequency condition for Experiment 1 (where all audits were computerized and all feedback was communicated by computer) is used as the Computerized System Mode / Computer Communication Feedback Mode cell in Experiment 2.

no interaction among participants[19]. As in Experiment 1, participants had an average age range of 20 to 29. Also similar to Experiment 1, the ratio of males to females was 52:44.[20]

4.3.2 Design: System Mode and Communication Feedback Mode

Experiment 2 is a 2 x 2 between-subjects design to test H2a, H2b, H3a and H3b by comparing the effects of varying System Mode (Manual, Computerized) and Communication Feedback Mode (Human, Computer) on the dependent variables.[21] Panel B of Table 2 illustrates the experimental design matrix and the cells tested in Experiment 2.

H2a examines the effect of the independent variable System Mode on the dependent variable Perceived Opportunity to commit fraud, while H2b examines the same independent variable's effect on the dependent variable Fraud Percentage. H3a examines the effect of the independent variable Communication Feedback Mode on the dependent variable Feeling When Caught fraudulently reporting, while H3b examines the same independent variable's effect on the dependent variable Fraud Percentage.

The dependent variables Perceived Opportunity and Fraud Percentage were previously described in the subchapter on the design for Experiment 1. The dependent variable Feeling When Caught is measured using the eleven-point scale question "For those periods in which you reported differently from the actual item collected and you were audited, how did you feel when

---

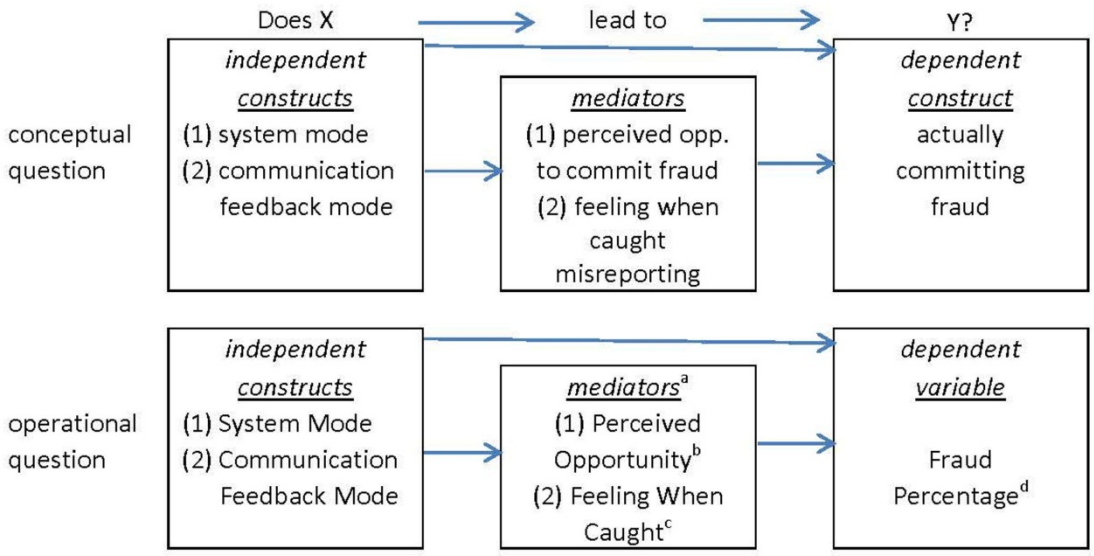
[19] In the sessions for two of the cells, 20 periods were completed, like in Experiment 1. In the sessions for the other two cells, 15 or 16 periods per session were completed. To avoid creating conditions that would be conducive to end-of-game behavior, participants were not informed of the planned number of periods beforehand.

[20] Post-experimental statistical analyses showed no significant differences across gender.

[21] Audit Frequency and Actual Detection Probability, both of which are manipulated in Experiment 1, are held constant in Experiment 2 – at Continuous Audit Frequency and Low 15% Actual Detection Probability.

you learned the audit results?" as shown in Appendix E. The question is designed on a scale ranging from 0=[felt very good] to 10=[felt very bad].

Figure 3 portrays the conceptual constructs and corresponding operational variables for Experiment 2, and Panel B of Table 2 illustrates the corresponding experimental design matrix and cells tested.



[a] The first mediator variable is the dependent variable in H2a and the second mediator variable is the dependent variable in H3a. It is hypothesized that the dependent variables in H2a and H3a mediate the effect on the other dependent variable, Fraud Percentage, in H2b and H3b, respectively.

[b] Perceived Opportunity is measured using participants' answers to the post-experimental question on perceived probability of detection: "What do you believe was the likelihood of being audited in any period?" Answers on an 11-point scale range from "no chance of being audited" (0 on the scale) to "very high likelihood of being audited" (10 on the scale). Because perceived opportunity to commit fraud is inversely related to the perceived probability of detection, I calculate Perceived Opportunity by subtracting the perceived probability of detection from 10.

[c] Feeling When Caught is measured using participants' answers to the post-experimental question "For those periods in which you reported differently from the actual item collected and you were audited, how did you feel when you learned the audit results?" Answers on an 11-point scale range from "felt very good" (0 on the scale) to "felt very bad" (10 on the scale).

[d] Fraud Percentage = (the number of fraudulent reports submitted) ÷ (the number of opportunities to benefit from reporting fraudulently if not caught).

Figure 3 Experimental Design for Experiment 2 (H2a, H2b, H3a, and H3b)

*Also see Table 2, Panel B which shows an experimental design matrix that summarizes the operationalization of the cells that are tested in Experiment 2.

4.3.2.1 Task

Experiment 2 uses the same experimental task as in Experiment 1, except that it varies the System Mode between Manual and Computerized (whereas in Experiment 1 it is fixed as Computerized), and varies the Communication Feedback Mode between Human and Computer (whereas in Experiment 1 it is fixed as Computer). In the Manual System Mode environment, the participant performs the task on paper and audits are performed manually by a human auditor: the human auditor manually audits a paper-based Report Form submitted by the participant.[22] This differs from the Computerized System Mode, in which the participant performs the task on the computer and audits are performed by a computerized audit program, as occurs throughout Experiment 1. The paper-based Report Form is simply the paper version of the same electronic Report Form used in the Computerized System Mode.

Communication Feedback Mode is the method of communicating audit results. In the Human Communication Feedback Mode the results of the audit are presented to the participant by a human, i.e., face-to-face. This differs from the Computer Feedback Mode, in which results are communicated to the participant via computer, i.e., on the participant's computer screen, as occurs throughout Experiment 1.

To preserve participants' anonymity, neither the experimenter who serves as the human auditor (in the System Mode - Manual condition) nor the experimenter who serves as the human

[22] See Appendix C.

feedback communicator (in the Communication Feedback Mode - Human condition) have a previous relationship with any of the participants, e.g., such as having served as their instructor.

4.3.2.2 Parameters

Experiment 2 uses the same experimental parameters as Experiment 1, except that the probability of being caught reporting fraudulently is held constant at 15%.

4.3.2.3 Random Lottery Incentive Mechanism

Experiment 2 uses the same random lottery incentive mechanism as Experiment 1.

5.0 EXPERIMENTAL RESULTS

This chapter presents the results of my hypothesis testing based on the data that I collected in the two experiments. I start by describing a pilot study that I conducted prior to collecting full sample size data. I then discuss the main results for Experiment 1 and Experiment 2.

5.1 PILOT STUDY

I conducted a pilot study to collect small samples across several experimental cells to determine which factors to include in my main experiments. I used the experimental design described in subchapter 4.2.2, and depicted in Panel A of Table 2, and varied the factor Audit Probability Information Provided because I was uncertain about the effect of providing actual audit detection probability information to participants. I varied Audit Probability Information Provided at three levels (Actual Probability, Actual Range, No Probability Provided). I also manipulated the Actual Detection Probability at three levels (High 85%, Medium 50%, and Low 15%).[23]

Because my pilot study indicated that the results under the Audit Probability Provided conditions were similar, I decided to use only the No Probability Provided condition in my main

[23] The Actual Range information provided to participants was a band spanning 15 percentage points that included the Actual Detection Probability point. For each level of Actual Detection Probability the corresponding ranges were: Low 5% to 20%; Medium 40% to 55%; High 85% to 90%.

experiments. That is, in my experiments, I did not provide participants with any information about the actual detection probability. Pilot study results also indicated the High and Medium conditions were similar, so for the main experiments I eliminated the Medium 50% level. In Experiment 1, I manipulated Actual Detection Probability at the other two levels, High 85% and Low 15%, as indicated in Panel A of Table 2, and in Experiment 2, I held Actual Detection Probability constant at the Low 15% level.

5.2 EXPERIMENT 1 RESULTS[24]

My first pair of hypotheses, H1a and H1b, predict an interaction between the independent variables Audit Frequency and Actual Detection Probability, as illustrated in Panel A and Panel B of Figure 1, respectively. The results in Panel A of Table 5 show that when the Actual Detection Probability is high the mean Perceived Opportunity is 1.71 for Continuous Audit and 2.19 for Periodic Audit. When the Actual Detection Probability is low the mean Perceived Opportunity is 6.90 for Continuous Audit and 5.88 for Periodic Audit. The pattern of these means is consistent with H1a, as graphically presented in Figure 4.

[24] The results reported for Experiment 1 are based on ANOVA, which makes certain assumptions about the data. One of the assumptions is that the dependent variable error term is normally distributed. This normality test was not met in several of my ANOVA tests. I ran corresponding Mann-Whitney non-parametric tests and compared the results to those of the ANOVA. Because I reach the same statistical inferences for all tests, I only report ANOVA results for Experiment 1.

Table 5 Test of H1a

Panel A: Descriptive Statistics - Mean (Standard Error)
DV: Perceived Opportunity

		Audit Frequency		
		Continuous	Periodic	
Actual Detection Probability	High (85%)	**1.71*** (0.37)	**2.19*** (0.37)	**1.95** (0.26)
	Low (15%)	**6.90*** (0.37)	**5.88*** (0.37)	**6.39** (0.26)
		4.30 (0.26)	**4.03** (0.26)	

*n=24 for all cells

Panel B: ANOVA Table
DV: Perceived Opportunity

	SS	df	MS	F	**p**	η_p^2 *
Audit Frequency	1.76	1	1.76	0.53	**0.47**	0.01
Actual Detection Prob.	472.59	1	472.59	141.63	**0.00**	0.61
Audit Freq. x Act. Det. Prob.	13.50	1	13.50	4.05	**0.05**	0.04
Error	306.98	92	3.34			
Total	794.83	95				

Panel C: Simple Main Effects Analyses (DV: Perceived Opportunity)

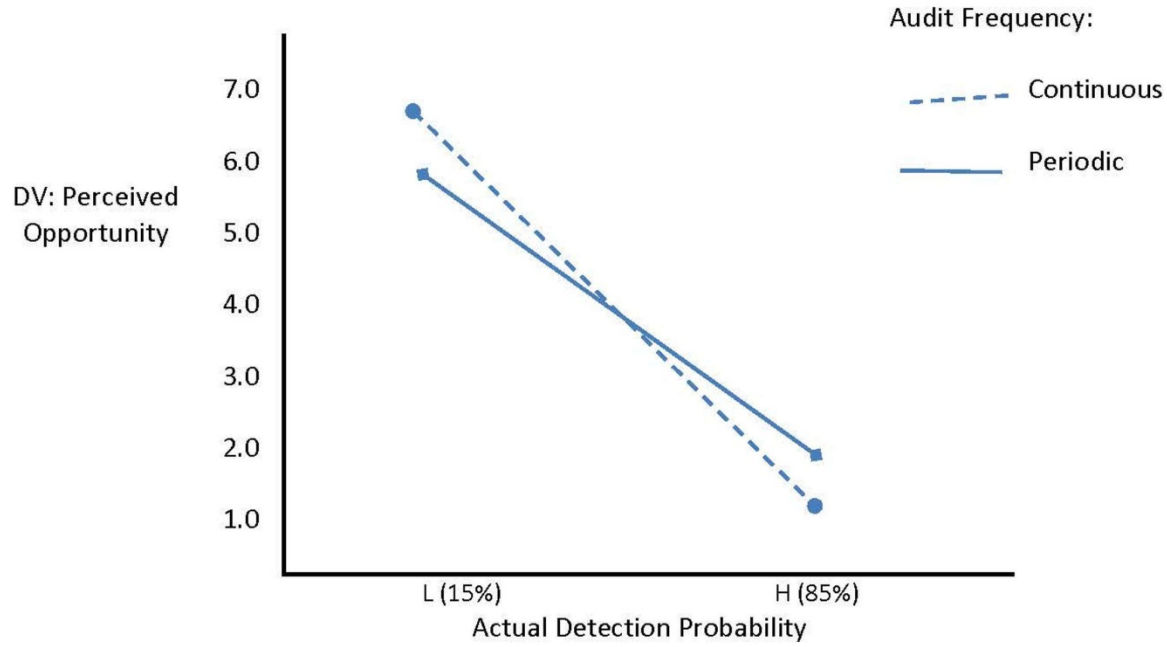
SME analysis: Actual Detection Probability = High

Audit Frequency			difference	F statistic	**p**	η_p^2
Continuous	v.	Periodic	0.48	0.83	**0.37**	.01

SME analysis: Actual Detection Probability = Low

Audit Frequency			difference	F statistic	**p**	η_p^2
Continuous	v.	Periodic	-1.02	3.75	**0.06**	.04

* Partial eta squared (η_p^2) is a measure of effect size, i.e., the strength of the relationship between two variables. In general: (1) a value of η_p^2 = 0.010 is considered a small effect size; (2) a value of η_p^2 = 0.059 is considered a medium effect size; and (1) a value of η_p^2 = 0.138 is considered a large effect size (Cohen 1992).



Note: Perceived Opportunity is measured using participants' answers to the post-experimental question on perceived probability of detection, stated as "What do you believe was the likelihood of being audited in any period?" Answers on an 11-point scale range from "no chance of being audited" (0 on the scale) to "very high likelihood of being audited" (10 on the scale). Because perceived opportunity to commit fraud is inversely related to the perceived probability of detection, Perceived Opportunity is calculated by subtracting the perceived probability of detection from 10.

Figure 4 Graphical Results of H1a

As shown in the 2x2 ANOVA presented in Panel B of Table 5, there is a significant interaction between Audit Frequency and Actual Detection Probability on Perceived Opportunity ($F(1,92) = 4.05$, $p = .05$),[25] consistent with H1a. To gain more insight into this effect, I performed simple main effect analyses of Audit Frequency at each level of Actual Detection Probability. The results of these tests, presented in Panel C of Table 5, show a marginally significant difference between Continuous Audit and Periodic Audit at the Low Actual Detection

[25] All of my p-values are reported based on the F-test in the ANOVA table. I do not report one-tailed p-values corresponding to t-tests even when I have directional predictions.

Probability level ($F(1,92) = 3.75$, $p = .06$) and no significant difference between the Continuous Audit and Periodic Audit at the High Actual Detection Probability level ($F(1,92) = .83$, $p = .37$). The significant interaction indicates that the difference between the Continuous Audit environment and the Periodic Audit environment is greater at the Low Actual Detection Probability level than at the High level.

Also, as one would expect, there is a significant main effect of the Actual Detection Probability because participants perceived more opportunity to commit fraud ($F(1,92) = 141.63$, $p < .001$) when there was a low Actual Detection Probability (mean = 6.39) than when there was a high Actual Detection Probability (mean = 1.95). The main effect of Audit Frequency on Perceived Opportunity is not significant in the ANOVA ($F(1,92) = .53$, $p = .47$) because its effect depends on the level of Audit Detection Probability, as evidenced by the significant interaction discussed above.

In H1b, Fraud Percentage is the dependent variable. Panel A of Table 6 presents the cell means, which are presented graphically in Figure 5. Once again, participants responded to the Actual Detection Probability as expected in that there is a significant main effect ($F(1,92) = 5.11$ $p = .03$) of the low Actual Detection Probability on Fraud Percentage (mean = 41%) resulting in more fraud ($F(1,92) = 5.11$, $p = .03$) than the high Actual Detection Probability (mean = 28%). However, when the Actual Detection Probability is high, Fraud Percentage is almost the same for Continuous Audit (mean = 28%) and Periodic Audit (mean = 27%). Similarly, when the Actual Detection Probability is low, Fraud Percentage is the same for Continuous Audit (mean = 41%) and for Periodic Audit (mean = 41%). As shown in Panel B of Table 6, there is no significant interaction ($F(1,92) = .00$, $p = .95$), and there is no significant main effect of Audit Frequency on Fraud Percentage ($F(1,92) = .02$, $p = .90$). Thus, I find no support for H1b.

Table 6 Test of H1b

Panel A: Descriptive Statistics - Mean (Standard Error)
DV: Fraud Percentage

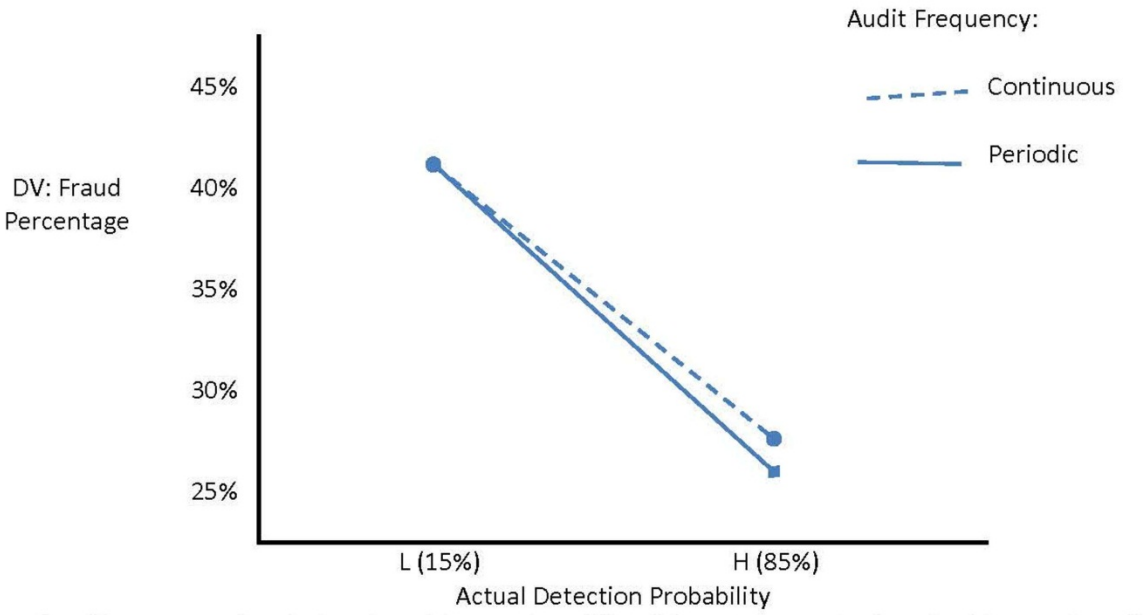
		Audit Frequency		
		Continuous	Periodic	
Actual Detection Probability	High (85%)	**28%*** (6)	**27%*** (6)	**28%** (4)
	Low (15%)	**41%*** (6)	**41%*** (6)	**41%** (4)
		35% (4)	**34%** (4)	

*n=24 for all cells

Panel B: ANOVA Table
DV: Fraud Percentage

	SS	df	MS	F	**p**	η_p^2 *
Audit Frequency	0.00	1	0.00	0.02	**0.90**	0.00
Actual Detection Prob.	0.44	1	0.44	5.11	**0.03**	0.05
Audit Freq. x Act. Det. Prob.	0.00	1	0.00	0.00	**0.95**	0.00
Error	8.00	92	0.09			
Total	8.45	95				

* Partial eta squared (η_p^2) is a measure of effect size, i.e., the strength of the relationship between two variables. In general: (1) a value of η_p^2 = 0.010 is considered a small effect size; (2) a value of η_p^2 = 0.059 is considered a medium effect size; and (1) a value of η_p^2 = 0.138 is considered a large effect size (Cohen 1992).



Note: Fraud Percentage is calculated as: (the number of fraudulent reports submitted) ÷ (the number of opportunities to benefit from reporting fraudulently if not caught).

Figure 5 Graphical Results of H1b

The overall results for Experiment 1 indicate that, consistent with H1a, the perceived opportunity to commit fraud in a Continuous Auditing system versus a Periodic Auditing system depends on the Actual Detection Probability, and when the Actual Detection Probability is low, a Continuous Audit can increase perceived fraud opportunity. However, this effect on individuals' perceptions did not translate into the effect on Fraud Percentage that was predicted in H1b.

5.3 EXPERIMENT 2 RESULTS[26]

Experiment 2 tests H2a and H2b, which predict main effects of System Mode, and H3a and H3b, which predict main effects of Communication Feedback Mode. As with the hypotheses tested in Experiment 1, part "a" in each pair of hypotheses predicts an effect on perceptions, and part "b" predicts a resulting effect on participants' fraud behavior.

H2a predicts that a Computerized System Mode will result in a higher Perceived Opportunity to commit fraud than a Manual System Mode. Panel A of Table 7 presents the cell means and Figure 6 depicts them graphically. As shown in Panel A of Table 7, Perceived Opportunity for the Computerized System Mode (mean = 6.79) is directionally lower than the Perceived Opportunity for the Manual System Mode (mean = 7.22). However, the 2X2 ANOVA presented in Panel B of Table 7 shows that the difference between these means is not statistically significant ($F(1,92) = 1.69$, $p = .20$). Therefore, I do not find support for H2a.

[26] The results reported for Experiment 2 are based on ANOVA, which makes certain assumptions about the data. One of the assumptions is that the dependent variable error term is normally distributed. This normality test was not met in several of my ANOVA tests. I ran corresponding Mann-Whitney non-parametric tests and compared the results to those of the ANOVA. Because I reach the same statistical inferences for all tests, I only report ANOVA results for Experiment 2.

Table 7 Test of H2a

Panel A: Descriptive Statistics - Mean (Standard Error)
DV: Perceived Opportunity

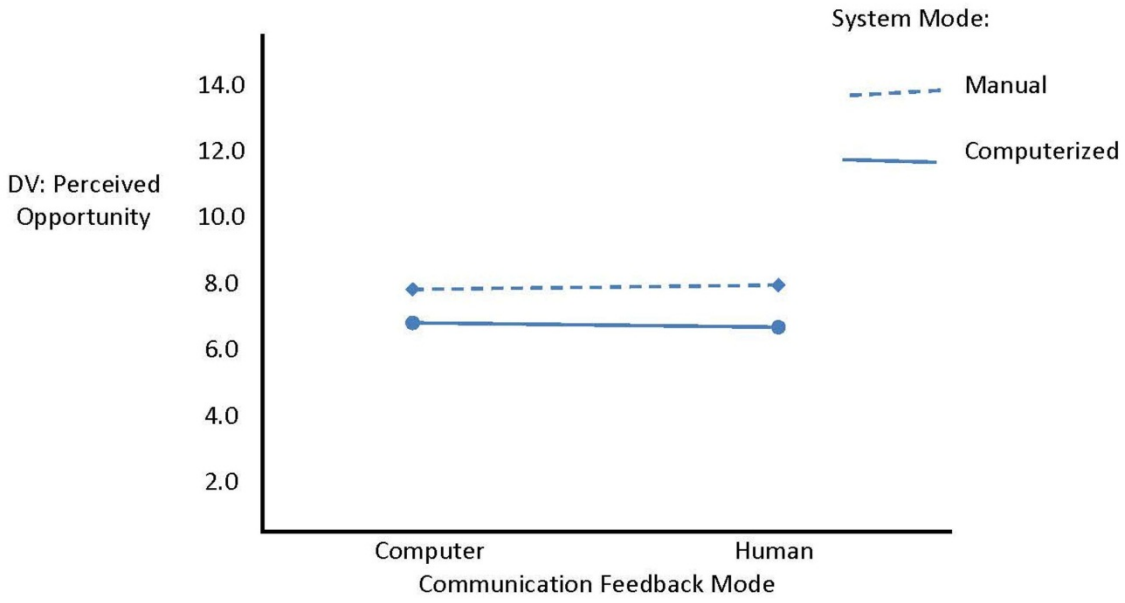
		System Mode		
		Manual	Comp	
Communication Feedback Mode	Human	**7.35** (0.33)	**6.69** (0.33)	**7.02** (0.23)
	Computer	**7.08** (0.33)	**6.90** (0.33)	**6.99** (0.23)
		7.22 (0.23)	**6.79** (0.23)	

*n=24 for all cells

Panel B: ANOVA Table
DV: Perceived Opportunity

	SS	df	MS	F	**p**	η_p^2 *
System Mode	4.38	1	4.38	1.69	**0.20**	0.02
Comm. Feedback Mode	0.02	1	0.02	0.01	**0.92**	0.00
Sys. Mode x CFB Mode	1.38	1	1.38	0.53	**0.47**	0.01
error	237.97	92	2.59			
total	243.75	95				

* Partial eta squared (η_p^2) is a measure of effect size, i.e., the strength of the relationship between two variables. In general: (1) a value of η_p^2 = 0.010 is considered a small effect size; (2) a value of η_p^2 = 0.059 is considered a medium effect size; and (1) a value of η_p^2 = 0.138 is considered a large effect size (Cohen 1992).



Note: Perceived Opportunity is measured using participants' answers to the post-experimental question on perceived probability of detection, stated as "What do you believe was the likelihood of being audited in any period?" Answers on an 11-point scale range from "no chance of being audited" (0 on the scale) to "very high likelihood of being audited" (10 on the scale). Because perceived opportunity to commit fraud is inversely related to the perceived probability of detection, Perceived Opportunity is calculated by subtracting the perceived probability of detection from 10.

Figure 6 Graphical Results of H2a

H2b predicts that a Computerized System Mode will result in a lower Fraud Percentage than a Manual System Mode. Panel A of Table 8 reports the cell means and Figure 7 depicts them graphically. The Fraud Percentage for the Computerized System Mode (mean = 36%) is directionally lower than that of the Manual System Mode (mean = 42%), but as was the case for H2a, the 2X2 ANOVA presented in Panel B of Table 8 indicates that the difference between these means is not statistically significant ($F(1,92) = .76$, $p = .38$). Thus, I do not find support for H2b.

Table 8 Test of H2b

Panel A: Descriptive Statistics - Mean (Standard Error)
DV: Fraud Percentage

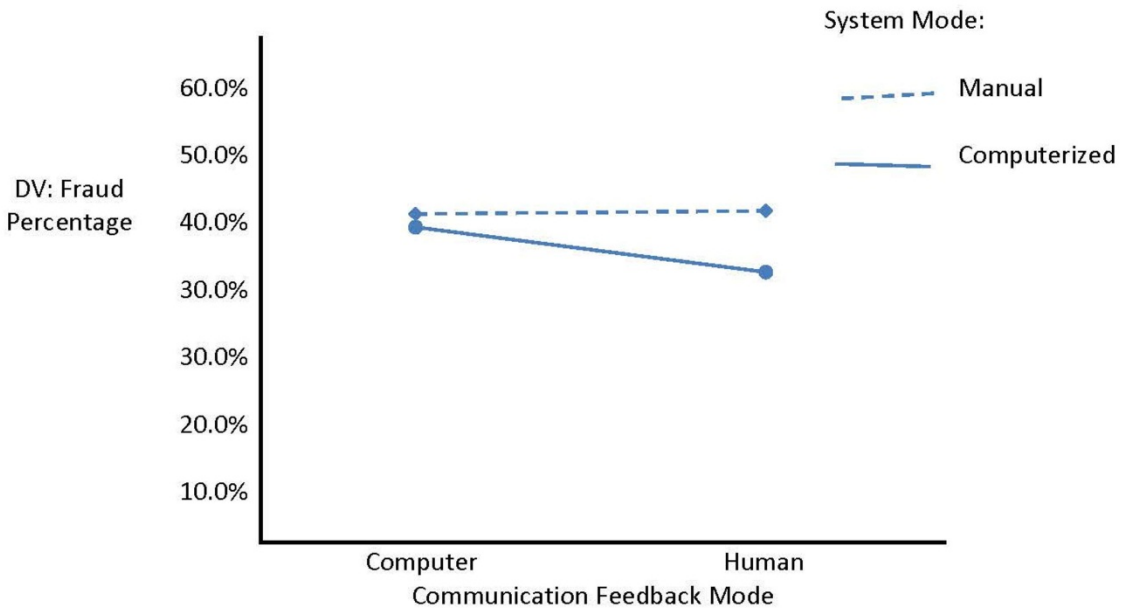
		System Mode		
		Manual	Comp	
Communication Feedback Mode	Human	**43%*** (7)	**31%*** (7)	**37%** (5)
	Computer	**41%*** (7)	**41%*** (7)	**41%** (5)
		42% (5)	**36%** (5)	

*n=24 for all cells

Panel B: ANOVA Table
DV: Fraud Percentage

	SS	df	MS	F	**p**	η_p^2 *
System Mode	0.08	1	0.08	0.76	**0.38**	0.01
Comm. Feedback Mode	0.04	1	0.04	0.35	**0.56**	0.00
Sys. Mode x CFB Mode	0.09	1	0.09	0.84	**0.36**	0.01
Error	9.70	92	0.11			
Total	9.90	95				

* Partial eta squared (η_p^2) is a measure of effect size, i.e., the strength of the relationship between two variables. In general: (1) a value of η_p^2 = 0.010 is considered a small effect size; (2) a value of η_p^2 = 0.059 is considered a medium effect size; and (1) a value of η_p^2 = 0.138 is considered a large effect size (Cohen 1992).



Note: Fraud Percentage is calculated as: (the number of fraudulent reports submitted) ÷ (the number of opportunities to benefit from reporting fraudulently if not caught).

Figure 7 Graphical Results of H2b

My final pair of hypotheses, H3a and H3b, predicts main effects for Communication Feedback Mode, where part "a" predicts an effect on perceptions and part "b" predicts a resulting effect on participants' fraud behavior. H3a predicts that a potential fraud perpetrator will feel more uncomfortable receiving feedback about having attempted a fraud if that feedback is communicated face-to-face by a human than if the feedback is communicated via computer. Panel A of Table 9 presents the cell means, and Figure 8 presents these results graphically. As shown in the ANOVA results reported in Panel B of Table 9, the Feeling When Caught in the Human Communication Feedback Mode (mean = 5.58) is marginally greater than ($F(1,73) = 3.70$, $p = .06$) in the Computer Communication Feedback Mode (mean = 4.38), providing modest support for H3a.

Table 9 Test of H3a

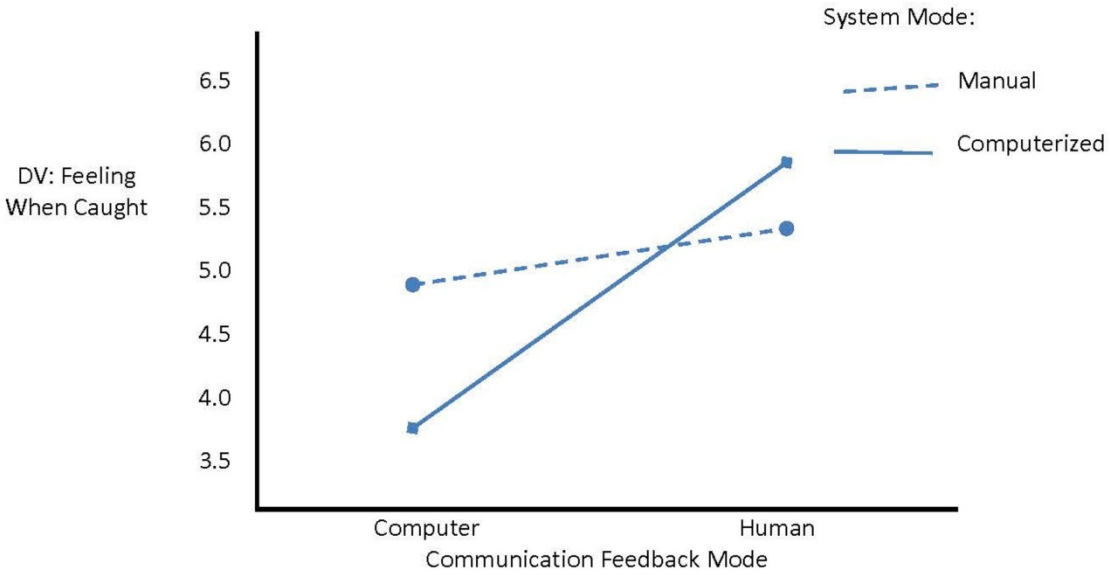
Panel A: Descriptive Statistics - Mean (Standard Error)
DV: Feeling When Caught

		System Mode		
		Manual	Comp	
Communication Feedback Mode	Human	**5.43**	**5.76**	**5.58**
		(0.61)	(0.66)	(0.45)
		n=20	n=17	n=37
	Computer	**4.95**	**3.86**	**4.38**
		(0.62)	(0.59)	(0.43)
		n=19	n=21	n=40
		5.19	**4.71**	
		(0.43)	(0.44)	
		n=39	n=38	

Panel B: ANOVA Table
DV: Feeling When Caught

	SS	df	MS	F	**p**	η_p^2 *
System Mode	2.69	1	2.69	0.37	**0.55**	0.00
Comm. Feedback Mode	27.21	1	27.21	3.70	**0.06**	0.05
Sys. Mode x CFB Mode	9.78	1	9.78	1.33	**0.25**	0.02
error	536.72	73	7.35			
total	577.59	76				

* Partial eta squared (η_p^2) is a measure of effect size, i.e., the strength of the relationship between two variables. In general: (1) a value of η_p^2 = 0.010 is considered a small effect size; (2) a value of η_p^2 = 0.059 is considered a medium effect size; and (1) a value of η_p^2 = 0.138 is considered a large effect size (Cohen 1992).



Note: Feeling When Caught is measured using participants' answers to the post-experimental question "For those periods in which you reported differently from the actual item collected and you were audited, how did you feel when you learned the audit results?" Answers on an 11-point scale range from "felt very good" (0 on the scale) to "felt very bad" (10 on the scale).

Figure 8 Graphical Results of H3a

H3b predicts that the Human Communication Feedback Mode will result in a lower Fraud Percentage among potential fraud perpetrators than does the Computer Communication Feedback Mode. Panel A of Table 8 presents the cell means, and Figure 7 presents these results graphically. As shown in the ANOVA results reported in Panel B of Table 8, the Fraud Percentage in the Human Communication Feedback Mode (mean = 37%) is not different from ($F(1,92) = .35$, $p = .56$) the Fraud Percentage in the Computer Communication Feedback Mode (mean = 41%). Thus, the results do not support H3b.

Table 10 summarizes the results of the tests of my hypotheses reported above.

Table 10 Summary of Hypothesis Testing Results

	perceptions		behavior
Experiment	DV = Perceived Opportunity	DV = Feeling When Caught	DV = Fraud Percentage
1	H1a supported (p<.05)		H1b not supported
2	H2a not supported		H2b not supported
2		H3a part. supp. (p<.10)	H3b not supported

6.0 DISCUSSION AND CONCLUSIONS

Advancements in information technology have allowed organizations and their auditors to automate many of their operations. However, computerization has also introduced new challenges and increased some types of fraud risks. A fraud risk management tool that has gained in popularity is computerized continuous auditing. It is commonly accepted by practitioners that continuous auditing provides increased audit coverage, efficiency, and effectiveness, and thereby increases the control system's ability to detect, prevent, and deter fraud. There is very little academic accounting research that investigates the effectiveness of continuous auditing on fraud, and the little there is suggests that continuous auditing is generally an effective fraud deterrent. I rely on theory from psychology, criminology, and information systems to design a study that examines different aspects of continuous auditing in order to (1) determine which aspects make it effective at deterring fraud, and (2) identify circumstances in which continuous auditing can be less effective at deterring fraud.

Continuous auditing is typically incorporated into a computerized environment. An advantage of using the experimental method in this study is that it allows me to disentangle effects that occur simultaneously in actual organizations in order to determine which specific aspects of the natural environment influence the perceived opportunity to commit fraud. My study extends previous work in this area (i.e., Hunton et al. 2008, 2010) in several ways. First, I

disentangle the components of a continuous audit environment by manipulating audit frequency, actual detection probability, system mode, and communication feedback mode separately. Second, my design creates an environment in which participants perform the same task multiple times, allowing them to actually experience the task and receive feedback on the results. Third, I provide an incentive compensation structure in which earnings are based on a combination of participant's choices and random outcomes, thereby establishing an environment in which decision-making has an actual financial consequence. As will be discussed further later, my study also adds insights into our understanding of the role of the fraud triangle.

In my first experiment, I varied the actual fraud detection probability and find that a continuous audit's relative effectiveness, compared to a periodic audit, depends on whether there is a high or low actual fraud detection probability. In my second experiment, I held constant the actual audit detection probability and used a continuous audit approach, but varied two other components of the continuous audit environment to determine what role they play in a continuous audit system's effectiveness. Specifically, I varied the system mode to determine whether a continuous manual detection system versus a continuous computerized detection system influences the system's effectiveness at fraud deterrence. I also varied whether the audit results are communicated to a potential fraud perpetrator via computer-mediated feedback or are communicated face-to-face by a human in order to determine whether participants would feel worse about receiving feedback from a human, and therefore, be less likely to commit fraud.

I find that the effectiveness of continuous auditing at reducing the perceived opportunity to commit fraud depends on the overall actual probability of detecting fraud, and that when that actual fraud detection probability is low, a continuous audit results in a higher perceived opportunity to commit fraud than does a periodic audit. This is an important finding because the

actual fraud detection probability in organizations is often lower than desirable. As technology evolves, so do new fraud schemes. Thus, auditors must be imaginative enough to anticipate these new fraud schemes in their continuous audit plan. However, because no continuous audit plan can anticipate all possible fraud schemes, continuous auditing can never be 100% effective in preventing and detecting fraud. It is crucial that internal auditors understand the circumstances under which continuous audits are effective at deterring fraud, and that they understand when continuous auditing can actually be less effective than periodic auditing at deterring fraud.

My results also show that there is no difference in effectiveness of a manual versus computerized detection system, indicating that this is not the critical aspect of the computerized continuous audit environment. My hypothesis testing results yielded a significance level that borders on marginal ($p = .20$) with a small effect size ($\eta_p^2 = .02$) in the predicted direction. This lack of a significant result may be because computer detection is truly not perceived as more effective than human detection or it could be attributable to my statistical tests not being powerful enough to detect this small effect. As mine is the first study to explore this issue, future research can investigate whether computer detection is a key aspect of the deterrent effect of a continuous computerized audit.

An interesting finding in my study is the very large effect ($\eta_p^2 = .61$) of actual detection probability. This large effect size suggests that there is a high benefit to an organization of increasing the probability of detecting fraud. This could be accomplished, for example, through greater resources dedicated to detecting fraud, or increased effectiveness in audit methods that reduces the chance of the audit system missing actual fraud, i.e., reducing detection risk. My study does not address how costly it would be for an organization to obtain this benefit of a higher actual detection probability, so I do not know which of these measures would be cost

effective to initiate on actual audits. However, this very large effect in the expected direction lends confidence that participants in my study attended to the experimental task and responded in a systematic and sensible manner (i.e., they did not respond randomly).

I also find marginal support (at p=.06) that potential fraud perpetrators feel worse about receiving face-to-face feedback about committing fraud than they do about receiving that feedback by computer. The fact that the effect size of this result is moderate ($\eta_p^2 = .05$), and larger than several of the study's other effects, indicates that this effect is worth exploring further in future research to determine if it replicates. If face-to-face feedback does create greater discomfort than computer-mediated communication, this would confirm the importance of human contact in an auditing environment.

While my experiments document differences in participants' perceptions of fraud opportunity and in their feelings about being caught misreporting, I do not find any change in their actual fraud behavior. In the fraud triangle, actual fraud behavior depends on the presence of all three sides of the fraud triangle (i.e., perceived opportunity, incentives/pressure, and attitude/rationalization). In my study, I held constant the incentives to commit fraud across treatment conditions, and measured the perceived opportunity to commit fraud as one of my dependent variables. However, I did not manipulate participants' attitudes or ability to rationalize committing fraud between treatment conditions. Attitude includes factors such as integrity and willingness to lie or misreport, which could differ among participants in my experiment. In a natural environment, potential fraud perpetrators are also deterred from committing fraud if they are unable to rationalize that their behavior is acceptable under the circumstances.

It is possible that the conditions in my experiment make it easier to rationalize committing fraud than it would be in the natural environment. Specifically, I intentionally avoid

using judgmental language such as “fraud” or “dishonesty” in my experimental materials. In addition, in my oral instructions I used neutral words and phrases such as: “In any period selected for audit if the item you reported is not the same as what you actually collected, and the auditor discovers a mismatch, you will be assessed a penalty.” In a setting with a richer fraud context there might be a larger effect size than I find in my more neutral, abstract setting. In future research, I plan to make the attitude/rationalization side of the fraud triangle more salient and examine if that affects fraud behavior. I plan to create experimental settings that increase the ethical component or the stigma attached to fraudulent behavior and explore how this influences participants’ propensity to misreport when given the opportunity.

One interesting result in my study relates to the effectiveness of the continuous auditing system when the actual probability of fraud detection is high. Recall that there is a significant interaction indicating that the effect of continuous versus periodic auditing differs between the high and low actual detection probability conditions, and that as predicted, continuous auditing results in a higher perceived opportunity to commit fraud when the actual probability of detection is low. In contrast, when there is a high actual probability of fraud detection, I predict that a continuous audit would be more effective and result in a lower perceived opportunity to commit fraud. While the direction of the means is consistent with my prediction, the simple main effect test indicates that there is no statistical difference between the perceived opportunity in the continuous and periodic audit conditions. I conjecture that this result might have occurred because there could be a “floor effect” on perceived opportunity in the high fraud detection condition, where the periodic and continuous audits are both highly effective at reducing perceived opportunity, resulting in very low assessments of perceived opportunity in both of these conditions. While it would be interesting to know which audit frequency type is more

effective when there is a high probability of fraud detection, I would argue that the more important case is when there is a low probability of fraud detection, because this is the riskier setting. My study is the first to identify a circumstance in which continuous audits are not perceived to be more effective than periodic audits.

The results of my study have important implications for designing control systems in practice. Specifically, internal auditors and other professionals aiming to decrease fraud risk should be aware that continuous auditing is not always more effective than periodic auditing. Because continuous auditing's effectiveness depends on the actual probability of fraud detection, auditors should work toward increasing the actual probability of detecting fraud by identifying more possible fraud schemes to include in their testing as part of their continuous audit plan. They also should be careful about abandoning the use of their traditional audit tests once they implement a continuous audit system, and could consider supplementing continuous audits with existing audit tests. Because my results indicate that potential fraud perpetrators feel worse when feedback is communicated in a face-to-face interaction than when it is communicated via a computer-mediated communication, organizations may want to consider combining their computerized continuous audit approach with a periodic audit involving a human auditor. Finally, my finding that reducing perceived opportunity to commit fraud does not always result in a reduction of fraudulent behavior suggests that organizations should not focus their fraud reduction efforts solely on the perceived opportunity side of the fraud triangle. Rather, they may want to also engage in activities that reduce potential perpetrator's ability to rationalize committing fraud, such as improving the organizations' control environment and tone at the top.

This study relies on the experimental method and, accordingly, has its accompanying limitations. One limitation is the extent to which the effects I observe in this study can be

expected to generalize to a real-world environment. I used an abstract setting with, as previously mentioned, a highly neutral ethical context; it is possible that the results would change in an experiment with a fraud context, which could bring out ethical considerations for participants. Two other design choices also limit my ability to generalize the results – my study probably includes fewer consequences of being caught and a higher likelihood that an audit will detect a fraud than would be the case in a real-world setting. Specifically, in my experiment the penalty was strictly monetary, whereas in the real world the consequences for fraud are more severe and include not only monetary consequences, such as loss of future earnings, but also loss of reputation and possibly time in prison. On the other hand, in my study audits are 100% effective, whereas in the real-world this is unlikely to be the case. On actual audits, the likelihood of getting away with a fraud would be based on not only the probability of being audited but also the probability of being detected if audited. While constraining my experiment in this way was necessary to achieve experimental control, it limits my ability to generalize my results to the real-world based only on the results on an initial study in this area.

APPENDIX A

EXPERIMENTAL PROCEDURES

Continuous Audit Condition

An experimental session for a Continuous Audit Treatment Condition is composed of these steps:

1. procedures explained to participants
2. participants sign consent form
3. experiment begins
4. participants receive notification of item collected
5. participants submit their report on item collected, amount collected, and their share of the amount collected
6. continuous audits performed for randomly selected participants/periods
7. individual audit results communicated to each participant
8. repeat steps 4 through 7 until end of interim period (first set of periods)
9. (intentionally left blank)
10. (intentionally left blank)
11. interim experimental questionnaire administered at end of interim period

12. repeat steps 4 through 7 until end of session (second set of periods)

13. experiment concluded by administering post-experimental questionnaire and making payments to participants.

Periodic Audit Condition

An experimental session for a Periodic Audit Treatment Condition is composed of these steps:

1. procedures explained to participants

2. participants sign consent form

3. experiment begins

4. participants receive notification of item collected

5. participants submit their report on item collected, amount collected, and their share of the amount collected

6. (intentionally left blank)

7. (intentionally left blank)

8. repeat steps 4 through 7 until end of interim period (first set of periods)

9. audits performed for selected participants/periods

10. individual audit results communicated to each participant

11. interim experimental questionnaire administered at end of interim period

12. repeat steps 4 through 7 until end of session (second set of periods)

13. experiment concluded by administering post-experimental questionnaire and making payments to participants.

Description of Steps

Step #1 Procedures Explained to Participants

Prior to beginning the experiment, the lead experimenter explains the nature of the experiment. A handout on "Information About This Experiment" is distributed to the participants (see Appendix A). The lead experimenter explains the experimental procedures to the participants. Participants' questions and comments are settled prior to beginning the experiment.

Step #2 Participants Sign Consent Form

IRB-approved consent forms are distributed to participants for their review and signature. Signed consent forms are collected.

Step #3 Experiment Begins

The experiment begins. Once the experiment has begun participants may not talk, make noise, make hand signals, or otherwise communicate or distract in any way.

Step #4 Participants Receive Notification of Item Collected (A or B)

Participants' computer screens show them an Item Collected form (Appendix B). The form lets the participant know which of the items, A or B, she collected. Each participant receives a unique form that includes their manager number and the period number. These forms are private; they are only to be seen by the participant, Nevertheless, while the Item Collected form is private, the information on the forms is available to the auditor for any participant/period selected for audit.

Step #5 Participants Submit Their Reports

Participants submit their reports indicating the item collected, amount collected, and amount they retain (Appendix C). They do so by entering their report on a computer screen that appears on their computer for the current period.

Step #6 Audits Performed for Selected Participants/Periods

In the continuous audit treatment conditions, audits are performed at the end of each period. Specific participants' periods are randomly selected for audit (for any given period, some but not all participants' reports are selected for audit[27]). The computerized audit program (or the human auditor in the human audit condition) audits the reports submitted by participants for those specific periods randomly selected for audit.

Step #7 Audit Results Communicated to Participants

In the continuous audit condition, audit results are communicated to the participant immediately after the audit. Participants are informed (1) whether they were audited for the period and, if so, (2) the results of the audit.

Step #9 Audits Performed for Selected Participants/Periods

In the periodic audit treatment conditions, audits are performed at the end of the interim period. Specific participants' periods are randomly selected for audit (for any given period, some

[27] To save time and to make the running of the experiment as efficient as possible, random selections are done beforehand.

but not all participants' reports are selected for audit[28]). The computerized audit program (or the human auditor in the human audit condition) audits the reports submitted by participants for those specific periods randomly selected for audit.

Step #10 Audit Results Communicated to Participants

In the periodic audit condition, audit results are communicated to the participant at the end of the interim period. Participants are informed (1) whether they were audited for the period and, if so, (2) the results of the audit.

Step #11 Interim Experimental Questionnaire Period

At the end of the interim period, roughly half-way through the total number of periods for the experiment, and undisclosed to participants beforehand, an interim period experimental questionnaire is administered to participants (Appendix D).

Step #13 PEQs, Wrap Up and Pay Participants

Upon completion of the experiment, a post-experimental questionnaire (PEQ) is completed by participants (Appendix E). The PEQ includes questions to measure the dependent variable perceived probability of detection as well as other questions, including questions on risk preferences, demographic and other questions. Immediately after the PEQ is administered, the experimenter paymaster pays participants according to their earnings during the experiment.

[28] Ibid.

APPENDIX B

ITEM COLLECTED

Period # _____ Manager Number: _____

the item you collected this period was:	Item A

APPENDIX C

REPORT FORM

Period # _____ Manager Number: _____

Circle one of these: the column for Item A or the column for Item B	item collected	Item A	Item B
	amount collected	$21.60	$21.60
	your share	$0.60	$5.40

+-+

[ ] Your report for this period was not audited.

[ ] Your report for this period was audited. The results of the audit were:

[ ] no changes

[ ] you collected Item A but you reported Item B; you have been charged $7.20

APPENDIX D

INTERIM EXPERIMENTAL QUESTIONNAIRE

What do you believe was the likelihood of being audited in any period?

0	1	2	3	4	5	6	7	8	9	10
no chance of being audited		**low chance of being audited**			**equal chance of being audited or not**		**high likelihood of being audited**			**very high likelihood of being audited**

APPENDIX E

POST EXPERIMENTAL QUESTIONNAIRE

1. What do you believe was the likelihood of being audited in any period?

0	1	2	3	4	5	6	7	8	9	10
no chance of being audited		**low chance of being audited**			**equal chance of being audited or not**			**high likelihood of being audited**		**very high likelihood of being audited**

2. For those periods in which you collected Item A (lower-paying item):

a. How often did you report Item B (higher-paying item)? _____

b. When you did, why did you do so? _____
_____
_____
_____
_____

c. When you did not, why did you not do so? _____
_____
_____
_____
_____

3. How concerned were you that if you reported differently from the actual item collected, an audit would catch this?

0 1 2 3 4 5 6 7 8 9 10

|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|

not at all concerned **slightly concerned** **neither concerned nor unconcerned** **fairly concerned** **very concerned**

4. For those periods in which you reported differently from the actual item collected and you were audited, how did you feel when you learned the audit results?

0 1 2 3 4 5 6 7 8 9 10

|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|

felt very good **felt somewhat good** **felt neither good nor bad** **felt somewhat bad** **felt very bad**

5. Please indicate your professional/educational status (check all that apply):

□ work full-time □ study full-time □ part-time work □ part-time student

□ undergraduate student □ graduate student □ in-between jobs

6. How many years of professional work experience do you have?

□ less than 5 years □ 5 to 10 years □ more than 10 years

7. Please indicate your gender and age bracket:

□ F □ M

□ 18 to 25 years □ 26 to 35 years □ 36 to 45 years □ 46 to 55 years □ 56 or more

(Post Experimental Questions for Measuring Risk Preference)

Beginning on the next page you are asked a series of questions about what you would choose between two choices. Please indicate your choice for each one.

8a. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
1/10 chance for $2.00, 9/10 chance for $1.60.	☐	1/10 chance for $3.85, 9/10 chance for $0.10.	☐

8b. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
2/10 chance for $2.00, 8/10 chance for $1.60.	☐	2/10 chance for $3.85, 8/10 chance for $.10.	☐

8c. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
3/10 chance for $2.00, 7/10 chance for $1.60.	☐	3/10 chance for $3.85, 7/10 chance for $.10.	☐

8d. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
4/10 chance for $2.00, 6/10 chance for $1.60.	☐	4/10 chance for $3.85, 6/10 chance for $.10.	☐

8e. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
5/10 chance for $2.00, 5/10 chance for $1.60.	☐	5/10 chance for $3.85, 5/10 chance for $.10.	☐

8f. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
6/10 chance for $2.00, 4/10 chance for $1.60.	☐	6/10 chance for $3.85, 4/10 chance for $.10.	☐

8g. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
7/10 chance for $2.00, 3/10 chance for $1.60.	☐	7/10 chance for $3.85, 3/10 chance for $.10.	☐

8h. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
8/10 chance for $2.00, 2/10 chance for $1.60.	☐	8/10 chance for $3.85, 2/10 chance for $.10.	☐

8i. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
9/10 chance for $2.00, 1/10 chance for $1.60.	☐	9/10 chance for $3.85, 1/10 chance for $.10.	☐

8j. Given a choice, which of the following two options would you choose?

Option A:		Option B:	
10/10 chance for $2.00, 0/10 chance for $1.60.	☐	10/10 chance for $3.85, 0/10 chance for $.10.	☐

BIBLIOGRAPHY

Adams, M. (1994). Agency Theory and the Internal Audit. *Managerial Auditing Journal* 9(8): 8-12.

Aizen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes* 50: 179-211.

Albrecht, C. (2008*)*. *Fraud and Forensic Accounting In a Digital Environment: White Paper for The Institute for Fraud Prevention*. Austin, TX: The Institute for Fraud Prevention, 2008.

Albrecht, C. , M. Kranacher and S. Albrecht (2008*)*. *Asset Misappropriation Research White Paper for the Institute for Fraud Prevention*. Austin, TX: The Institute for Fraud Prevention, 2008.

Albrecht, S. and D. Schmoldt (1995). Employee Fraud. *Business Horizons* July-August 1988: 16-18.

Albrecht, W. Steve, C. C. Albrecht, C. O. Albrecht, M. Zimbelman (2012). *Fraud Examination*. Mason, OH: South-Western Cengage Learning.

Alm, J. and M. McKee (2006). Audit Certainty, Audit Productivity, and Taxpayer. Compliance *National Tax Journal* 59(4): 801-816.

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

Anderson, A., A. Harris and J. Miller (1983). Models of Deterrence Theory. *Social Science Research* 12(3): 236-262.

Anderson, U. and R. Young (1988). Internal Audit Planning in an Interactive Environment. *Auditing: A Journal of Practice and Theory* 8(1): 23-42.

Andrews, L. and T. Gutkin (1991). The Effects of Human Versus Computer Authorship on Consumers' Perceptions of Psychological Reports. *Computers in Human Behavior* 7: 311-317.

Asare, S., R. Davidson and A. Gramling (2008). Internal Auditors' Evaluation of Fraud Factors in Planning an Audit: The Importance of Audit Committee Quality and Management Incentives. *International Journal of Auditing* 12: 181-203.

Association of Certified Fraud Examiners (ACFE) (2010). 2010 Report to the Nation on Occupational Fraud & Abuse.

Baiman, S. (1990). Agency research in managerial accounting: A second look. *Accounting, Organizations, and Society* 15: 341-371.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review* 3(3): 193-209.

Banerjee, D. , T. Cronan and T. Jones (1998). Modeling IT Ethics: A Study in Situational Ethics. *MIS Quarterly* 22(1): 31-60.

Baron, R. and D. Kenny (1986). The Moderator-Mediator Variable Distinction in Social Psychology Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology* 51(6): 1173-1182.

Barra, R. (2010). The Impact of Internal Controls and Penalties on Fraud. *Journal of Information Systems* 24(1): 1-21.

Beasley, M. and G. Jenkins (2003). The Relation of Information Technology and Financial Statement Fraud. *Journal of Forensic Accounting* IV: 217-232.

Beasley, M., J. Carcello, D. Hermanson, and P. Lapides (2000). Fraudulent Financial Reporting: Consideration of Industry Traits and Corporate Governance Mechanisms. *Accounting Horizons* 14(4): 441-454.

Bedard, J., D. Deis, M. Curtis, and J. Jenkins (2008). Risk Monitoring and Control in Auditing Firms: A Research Synthesis. *Auditing: A Journal of Practice & Theory* 27(1): 187-218.

Bible, L., L. Graham, and A. Rosman (2005). The Effect of Electronic Audit Environments on Performance. *Journal of Accounting, Auditing & Finance* 20(1): 27-42.

Bloomfield, R. (1999). Discussion of An Experimental Investigation of Auditor-Auditee Interaction under Ambiguity. *Journal of Accounting Research* 37 (Supplement): 157-165.

Bogardus, E. (1925). Social Distance and its Origin. *Journal of Applied Sociology* 9: 216-226.

Bracha, A., M. Menietti and L. Vesterlund (2011). Seeds to succeed? Sequential giving to public projects. *Journal of Public Economics* 95: 416-427.

Braun, R. (2000). The effect of time pressure on auditor attention to qualitative aspects of misstatements indicative of potential fraudulent financial reporting. *Accounting, Organizations and Society* 25: 243-259.

Brazel, J. , and C. Agoglia (2007). An Examination of Auditor Planning Judgements in a Complex Accounting Information System Environment. *Contemporary Accounting Research* 24(4): 1059-1083.

Brazel, J. , C. Agoglia and R. Hatfield (2004). Electronic versus Face-to-Face Review: The Effects of Alternative Forms of Review on Auditors' Performance. *The Accounting Review* 79(4): 949-966.

Brazel, J. , K. Jones and M. Zimbelman (2009). Using Nonfinancial Measures to Assess Fraud Risk. *Journal of Accounting Research* 47(5): 1135-1166.

Brazel, J., K. Jones and D. Prawitt (2010). Improving Fraud Detection: Do Auditors React to Abnormal Inconsistencies between Financial and Nonfinancial Measures? Working paper.

Brazel, J., T. Carpenter and J. Jenkins (2009). Auditors' Use of Brainstorming in the Consideration of Fraud: Evidence from the Field. Working Paper.

Buller, D. and J. Burgoon (1996). Interpersonal deception theory. *Communication Theory* 6: 203-242.

Burgoon, J., D. Buller and K. Floyd (2001). Does participation affect deception success? A test of the interactivity principle. *Human Communication Research* 27: 503-534.

Burnaby, P., M. Howe and B. Muehlmann (2010). Detecting Fraud in the Organization: An Internal Audit Perspective. Working paper.

Camerer, C. and R. Hogarth (1999). The Effects of Financial Incentives in Experiments: A Review and Capital-Labor-Production Framework. *Journal of Risk and Uncertainty* 19(1-3): 7-42.

Camerer, C. and M. Weber (1992). Recent Developments in Modeling Preferences: Uncertainty and Ambiguity. *Journal of Risk and Uncertainty* 5: 325-379.

Carcello, J., D. Hermanson, and K. Raghunandan (2005). Factors Associated with U.S. Public Companies' Investment in Internal Auditing. *Accounting Horizons* 19(2): 69-84.

Carmichael, D. (1970). Behavioral Hypotheses of Internal Control. *The Accounting Review* April 1970: 235-245.

Carpenter, T. (2007). Audit Team Brainstorming, Fraud Risk Identification, and Fraud Risk Assessment: Implications of SAS No. 99. *The Accounting Review* 82(5): 1119-1140.

Carpenter, T. and J. Reimers (2005). Unethical and Fraudulent Reporting: Applying the Theory of Planned Behavior. *Journal of Business Ethics* 60: 115-129.

Carpenter, T., T., J. Reimers and P. Fretwell (2009). Internal Auditors' Fraud Judgments: The Benefits of Brainstorming in Groups. Working Paper.

Cathcart, R. and G. Kapoor (2010). An Internal Audit Upgrade. *Internal Auditor* June 2010: 47-49.

Chan, D. and M. Vasarhelyi (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems* 12: 152-60.

Chang, M. (1998). Predicting Unethical Behavior: A Comparison of the Theory of Reasoned Action and the Theory of Planned Behavior. *Journal of Business Ethics* 17: 1825-1834.

Charness, G. and P. Kuhn (2010). Lab Labor: What Can Labor Economists Learn from the Lab? NBER Working Paper Series, Working Paper 15913. National Bureau of Economic Research.

Chow, C.. M. Hirst and M. Shields (1995). The Effects of Pay Schemes and Probabilistic Management Audits on Subordinate Misrepresentation of Private Information: An Experimental Investigation in a Resource Allocation Context. *Behavioral Research in Accounting* 7: 1-16.

Cohen, Jacob (1992). Statistics a power primer. *Psychology Bulletin* 112: 155–159.

Colombier, N., L. Boemont, Y. Loheac and D. Masclet (2008). Risk aversion: an experiment with self-employed workers and salaries workers. *Applied Economics Letters* 15: 791-795.

Cook, G. and L. Clements (2009). Computer-based Proactive Fraud Auditing Tools. *Journal of Forensic & Investigative Accounting* 1(2): 1-23.

Coram, P., C. Ferguson, R. Moroney (2008). Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud. *Accounting and Finance* 48: 543-559.

Cox, J. C., V. Sadiraj and U. Schmidt (2011). Paradoxes and Mechanisms for Choice under Risk. Experimental Economics Center, Working Paper 2011-07. Georgia State University.

Curtis, M. and E. Payne (2008). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. *International Journal of Accounting Information Systems* 9: 104-121.

Dacin, T. and P. Murphy (2009). Understanding and Preventing Unethical Conduct in Organizations: A Situation- and Affect-Based Fraud Framework. Working Paper.

D'Arcy, John, A. Hovav, and D. Galletta (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20(1): 79-98.

Deloitte (2007). Treading Water: The 2007 Technology, Media & Telecommunications Security Survey. USA: Deloitte.

DePaulo, B. and D. Kashy (1998). Everyday Lies in Close and Casual Relationships. *Journal of Personality and Social Psychology* 74(1): 63-79.

Dijkstra, J., W. Liebrand and E. Timminga (1998). Persuasiveness of Expert Systems. *Behavior & Information Technology* 17: 155-163.

Dowling, C. (2009). Appropriate Audit Support System Use: The Influence of Auditor, Audit Team, and Firm Factors. *The Accounting Review* 84(3): 771-810.

Duffield, G. and P. Grabosky (2001a). The Psychology of Fraud. *Trends and Issues*, Australian Institute of Criminology No. 199 March: 1-6.

Duffield, G. and P. Grabosky (2001b). The Psychology of Fraud. *Trends and Issues*, Australian Institute of Criminology No. 200 March: 1-7.

Erickson, M., J. Gibbs and G. Jensen (1977). The Deterrence Doctrine and the Perceived Certainty of Legal Punishments. *American Sociological Review* 42(2): 305-317.

Falkenberg, L. and I. Herremans (1995). Ethical Behaviours in Organizations: Directed by the Formal or Informal Systems? *Journal of Business Ethics* 14: 133-143.

Flowerday, S. and R. von Solms (2005). Continuous auditing: verifying information integrity and providing assurances for financial reports. *Computer Fraud & Security* July 2005: 12-16.

Flowerday, S., A. Blundell and R. von Solms (2006). Continuous auditing technologies and models: A discussion. *Computers & Security* 25: 325-331.

Friend, R., Y. Hafferty, and D. Bramel (1990). A puzzling misinterpretation of the Asch 'conformity' study. *European Journal Social Psychology* 20(1): 29-44.

Galletta, D., A. Durcikova, A. Everard, and B. Jones (2002). Cognitive Fit and an Intelligent Agent for a Word Processor: Should Users Take All That Advice? *Proceedings of the 36th Hawaii International Conference on System Sciences*.

Galletta, D., A. Durcikova, A. Everard, and B. Jones (2005). Does Spell-Checking Software Need a Warning Label? *Communications of the ACM* 48(7): 82-86.

George, J. and A. Robb (2008). Deception and Computer-Mediated Communication in Daily Life. *Communication Reports* 21(2): 92-103.

George, J., K. Marett, and P. Tilley (2004). Deception Detection Under Varying Electronic Media and Warning Conditions. *Proceedings of the 37th Hawaii International Conference on System Sciences*.

Gopal, R. and G. Sanders (1997). Preventive and Deterrent Controls for Software Piracy. *MIS Quarterly* 22(4): 441-469.

Hammersley, J. (2006). Pattern Identification and Industry-Specialist Auditors. The Accounting Review 81(2): 309-336.

Hancock, J., J. Thomas-Santelli and T. Ritchie (2004). Deception and design: The impact of communication technologies on lying behavior. *CHI* 2004 6: 129-134

Harrison, G., E. Johnson, M. McInnes and E. Rutstrom (2005). Risk Aversion and Incentive Effects: Comment. *American Economic Review* 95(3): 897-901.

Herath, T. and H. Rao (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47: 154-165.

Hermanson, D., B. Moran, C. Rossie and D. Wolfe (2006). Continuous Monitoring of Transactions to Reduce Fraud, Misuse, and Errors. *Journal of Forensic Accounting* VII: 17-30.

Hey, J. and J. Lee (2005). Do Subjects Separate (or Are They Sophisticated)? *Experimental Economics* 8: 233-265.

Hillison, W. , C. Pacini and D. Sinason (1999). The internal auditor as fraud-buster. *Managerial Auditing Journal* 14(7): 351-362.

Hoffman, V. and M. Zimbelman (2009). Do Strategic Reasoning and Brainstorming Help Auditors Change Their Standard Audit Procedures in Response to Fraud Risk? *The Accounting Review* 84(3): 811-837.

Hogan, C. , Z. Rezaee, R. Riley, Jr., and U. Velury (2008). Financial Statement Fraud: Insights from the Academic Literature. *Auditing: A Journal of Practice & Theory* 27(2): 231-252.

Hollinger, R. (1989). Dishonesty in the Workplace: A Manager's Guide to Preventing Employee Theft. Park Ridge, IL: London House Press.

Hollinger, R. and J. Clark (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. *Social Forces* 62(2): 398-418.

Holmstrom, B. (1979). Moral hazard and observability. *Bell Journal of Economics* 10(1): 74-91.

Holt, C. and S. Laury (2002). Risk Aversion and Incentive Effects. *American Economic Review* 92(5): 1644-1655.

Holton, C. and R. Fuller (2008). Unintended Consequences of Electronic Monitoring of Instant Messaging. *IEEE Transactions on Professional Communication* 51(4): 381-395.

Honaker, L., V. Hector and T. Harrell (1986). Perceived Validity of Computer versus Clinician-Generated MMPI Reports. *Computers in Human Behavior* 12: 77-83.

Hunton, J. (2002). Blending Information and Communication Technology with Accounting Research. *Accounting Horizons* 16(1): 55-67.

Hunton, J. (2002). The Impact of Digital Technology on Accounting Behavioral Research. *Advances in Accounting Behavioral Research* 5: 3-17.

Hunton, J. , A. Wright and S. Wright (2004). Continuous Reporting and Continuous Assurance: Opportunities for Behavioral Accounting Research. *Journal of Emerging Technologies in Accounting* 1: 91-102.

Hunton, J., E. Mauldin and P. Wheeler (2008). Potential Functional and Dysfunctional Effects of Continuous Monitoring. *The Accounting Review* 83(6): 1551-1569.

Hunton, J., E. Mauldin and P. Wheeler (2010). Continuous monitoring and the status quo effect. *International Journal of Accounting Information Systems* 11(3): 239-252.

Institute of Internal Auditors (IIA) (2009a). International Professional Practices Framework. Altamonte Springs, FL: The Institute of Internal Auditors.

Institute of Internal Auditors (IIA) (2009b). Managing the Business Risk of Fraud: A Practical Guide: Executive Summary, IIA, AICPA and ACFE.

Institute of Internal Auditors (IIA) (2009c). Fraud Prevention and Detection in an Automated World. Global Technology Audit Guide. December 2009, IIA.

Institute of Internal Auditors (IIA) (2009d). Internal Auditing and Fraud. Practice Guide. December 2009, IIA.

Jans, M., M. Alles and M. Vasarhelyi (2010). Process Mining of Event Logs in Auditing: Opportunities and Challenges. Working Paper.

Jensen, M. and W. Meckling (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics* 3: 305-360.

Kalbers, L. and T. Fogarty (1995). Professionalism and Its Consequences: A Study of Internal Auditors. *Auditing: A Journal of Practice & Theory* 14(1): 64-86.

Kagel, J. H. and A. E. Roth, eds. (1995). Handbook of Experimental Economics, Princeton University Press.

Kankanhalli, A., H. Teo, B. Tan and K. Wei (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management* 23(2): 139-154.

Kiesler, S. , J. Siegel and T. McGuire (1984). Social Psychological Aspects of Computer-Mediated Communication. *American Psychologist* 39(10): 1123-1134.

Kiesler, S., L. Sproull and K. Waters (1996). A Prisoner's Dilemma Experiment on Cooperation with People and Human-Like Computers. *Journal of Personality and Social Psychology* 70(1): 47-65.

Knapp, C. and M. Knapp (2001). The effects of experience and explicit fraud risk assessment in detecting fraud with analytical procedures. *Accounting, Organizations and Society* 26: 25-37.

KPMG International (KPMG, 2010). What is Driving Continuous Auditing & Continuous Monitoring Today? USA: KPMG International Cooperative.

Krambia-Kapardis, M., C. Christodoulou, and M. Agathocleous (2010). Neural networks: the panacea of fraud detection? *Managerial Auditing Journal* 25(7): 659-678.

Kuhn, J. and S. Sutton (2006). Learning from WorldCom: Implications for Fraud Detection through Continuous Assurance. *Journal of Emerging Technologies in Accounting* 3: 61-80.

Kuhn, J. and S. Sutton (2010). Continuous Auditing in ERP System Environments: The Current State and Future Directions. *Journal of Information Systems* 24(1): 91-112.

Laury, S. (2005). Pay One or Pay All: Random Selection of One Choice for Payment. Andrew Young School of Policy Studies, Research Paper Series, Working Paper 06-13. Georgia State University.

Lehmann, C., S. Ramamoorti and M. Weidenmeier Watson (2010). Maximized Monitoring. *Internal Auditor* June 2010.

Leonard, L. and R. Haines (2007). Computer-mediated group influence on ethical behavior. *Computers in Human Behavior* 23: 2302-2320.

Leonard, L., T. Cronan and J. Kreie (2004). What influences IT ethical behavior intentions - planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management* 42: 143-158.

Lerch, F., M. Prietula and C. Kulik (1997). The Turing effect: The nature of trust in expert systems advice. In Expertise in context: Human and machine, P. Feltovich, K. Ford, & R. Hoffman, eds.; Menlo Park, CA: AAAI Press.

Loftus, J. and T. Vermeer (2003). Technology, Fraud Auditing, and Liquor. *Journal of Forensic Accounting* IV: 307-310.

Loewenstein, G. (1999). Experimental Economics from the Vantage Point of Behavioural Economics. *The Economic Journal* 109: F25-F34.

Lynch, A. and M. Gomaa (2003). Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior. *International Journal of Accounting Information Systems* 4: 295-308.

Lynch, A., U. Murthy, and T. Engle (2009). Fraud Brainstorming Using Computer-Mediated Communication: The Effects of Brainstorming Technique and Facilitation. *The Accounting Review* 84(4): 1209-1232.

Masli, A. , G. Peters, V. Richardson, and J. Sanchez (2010). Examining the Potential Benefits of Internal Control Monitoring Technology. *The Accounting Review* 85(3): 1001-1034.

Meyer, D. and J. Meyer (2006). Measuring Risk Aversion. *Foundations and Trends in Microeconomics* 2(2): 107-203.

Mitchell, J. (2009). Psychological Type in a Forensic Sample of Incarcerated Males. *Journal of Psychological Type* 69(3): 42-49.

Moyes, G., P. Liu, R. Landry, and H. Vicdan (2006). Internal Auditors' Perceptions of the Effectiveness of Red Flags to Detect Fraudulent Reporting. *Journal of Accounting, Ethics & Public Policy* 6(1): 1-28.

Muir, B. (1994). Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. *Ergonomics* 37(11): 1905-1922.

Muir, B. and N. Moray (1996). Trust in automation: Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics* 39(3): 429-460.

Murdoch, K. (2002). Intrinsic motivation and optimal incentive contracts. *Rand Journal of Economics* 33(4): 650-671.

Murphy, P. (2008). The Attitude Toward and Rationalization of Fraudulent Financial Reporting. Working Paper.

Nagin, D. and G. Pogarsky (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology* 39(4): 865-891.

Naquin, C., T. Kurtzberg and L. Belkin (2010). The Finer Points of Lying Online: E-Mail Versus Pen and Paper. *Journal of Applied Psychology* 95(2): 387-394.

Nelson, M. and H. Tan (2005). Judgment and Decision Making Research in Auditing: A Task, Person, and Interpersonal Interaction Perspective. *Auditing: A Journal of Practice & Theory* 24 Supplement: 41-71.

Nelson, W. (1998). Reference Wealth Effects in Sequential Choice. *Journal of Risk and Uncertainty* 17: 27-47.

Nussenbaum, D. (2010). Three Approaches to Combatting Enterprise Fraud. Bank Systems & Technology January 22, 2010 [online] Available at http://www.banktech.com/blog/227100911 (February 14, 2011).

O'Donnell, E. and J. Smith-David (2000). How information systems influence user decisions: a research framework and literature review. *International Journal of Accounting Information Systems* 1: 178-203.

Pancer, S., M. George and R. Gebotys (1992). Understanding and Predicting Attitudes Towards Computers. *Computers in Human Behavior* 8: 211-222.

Park, R. (1924). The Concept of Social Distance As Applied to the Study of Racial Attitudes and Racial Relations. *Journal of Applied Sociology* 8: 339-344.

Plumlee, R. (1985). The Standard of Objectivity for Internal Auditors: Memory and Bias Effects. **Journal of Accounting Research** 23(2): 683-699.

Rae, K. and N. Subramaniam (2008). Quality of internal control procedures: Antecedents and moderating effect on organizational justice and employee fraud. *Managerial Auditing Journal* 23(2): 104-124.

Ramos, M. (2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy* January 2003: 28-36.

Rankin, F. , S. Schwartz and R. Young (2008). The Effect of Honesty and Superior Authority on Budget Proposals. *The Accounting Review* 83(4): 1083-1099.

Ratley, J. (2011). From the President and CEO. *Fraud Magazine* May/June 2011: 2.

Rezaee, Z. (2005). Causes, consequences, and deterrence of financial statement fraud. C*ritical Perspectives on Accounting* 16: 277-298.

Rezaee, Z., A. Sharbatoghlie, R. Elam and P. McMickle (2002). Continuous Auditing: Building Automated Auditing Capability. *Auditing: A Journal of Practice & Theory* 21(1): 147-163.

Richards, D. (2008). Presentation before The Institute of Internal Auditors (IIA) Pittsburgh Chapter, April 7, 2008.

Rieh, S. and D. Danielson (2007). Credibility: A Multidisciplinary Framework. *Annual Review of Information Science and Technology* 41: 307-364.

Roca, M. and A. Maule (2009). The effects of endowment on the demand for probabilistic information. *Organizational Behavior and Human Decision Processes* 109: 56-66.

San Miguel, J. and V. Govindarajan (1984). The Contingent Relationship Between The Controller and Internal Audit Functions in Large Organizations. *Accounting, Organizations and Society* 9(2): 179-188.

Shavell, S. (1979). Risk Sharing and Incentives in the Principal and Agent Relationship. *The Bell Journal of Economics* 10(1): 55-73.

Sheridan, T., T. Vamos and S. Aida (1983). Adapting Automation to Man, Culture and Society. *Automatica* 19(6): 605-612.

Shih, C. F., J. Dedrick and K. L. Kraemer (2005). Rule of Law and the International Diffusion of E-Commerce. *Communications of the ACM* 48(1): 57-62.

Siegel, J., V. Dubrovsky, S. Kiesler, and T. McGuire (1986). Group Processes in Computer-Mediated Communication. *Organizational Behavior and Human Processes* 37: 157-187.

Sinnett, W. (2009). Does Internal Control Improve Operations And Prevent Fraud? *Financial Executives Research Foundation Reflections on Research* 1944-2009: 32-36.

Snow, A. and R. Warren Jr. (2005). Ambiguity about audit probability, tax compliance, and taxpayer welfare. *Economic Inquiry* 43(4): 865-871.

Snow, A. and R. Warren Jr. (2007). Audit Uncertainty, Bayesian Updating, and Tax Evasion. *Public Finance Review* 35: 555-571.

Sproull, L. and S. Kiesler (1986). Reducing social context cues: Electronic mail in organizational communication. *Management Science* 32: 1492-1512.

Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research* 1(3): 255-276

Straub, D. and R. Welke (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* 22(4): 441-469.

Tosi, H.. J. Katz and L. Gomez-Mejia (1997). Disaggregating the agency contract: The effects of monitoring, incentive alignment, and term in office on agent decision making. *Academy of Management Journal* 40(3): 584-602.

Trotman, K., R. Simnett and A. Khalifa (2009). Impact of the Type of Audit Team Discussions' on Auditors' Generation of Material Frauds. *Contemporary Accounting Research* 26(4): 1115-1142.

Tseng, S. and B. Fogg (1999). Credibility and Computing Technology. *Communications of the ACM* 42(5): 39-44.

Turner, J., T. Mock and R. Srivastava (2003). An Analysis of the Fraud Triangle. Working Paper.

Urbaczewski, A. and L. Jessup (2002). Does electronic monitoring of employee Internet usage work? *Communications of the ACM* 45(1): 80-83.

Varma, K. and A. Doob (1998). Deterring economic crimes: the case of tax evasion. (Canada). *Canadian Journal of Criminology* 40(2): 165-184.

Vasarhelyi, M. and F. Halper (1989). The Continuous Audit of Online Systems. In *Artificial Intelligence in Accounting and Auditing*, M. Vasarhelyi, ed.; New York: Markus Wiener Publishers.

Vasarhelyi, M., A. Kogan and M. Alles (2002). Would Continuous Auditing Have Prevented the Enron Mess? *The CPA Journal* July 2002: 80.

Wells, J. (2001). Why Employees Commit Fraud. *Journal of Accountancy* February 2001: 89-91.

Wells, J. (2004). New Approaches to Fraud Deterrence. *Journal of Accountancy* February 2004: 72-76.

Wells, J. (2010). Principles of Fraud Examination, Hoboken, NJ: John Wiley & Sons, Inc.

Wells, J. (2008). The Real Secret to Fraud Deterrence. *The CPA Journal* June 2008: 6.

Wenzel, M. (2004). The Social Side of Sanctions: Personal and Social Norms as Moderators of Deterrence. *Law and Human Behavior* 28(5): 547-567

Wheeler, P. and R. Sriram (1997). The Information Criminologist: Litigation Services in EDP Environment. *Review of Accounting Information Systems* 1(3): 63-72.

Wheeler, P. and V. Arunachalam (2009). The effects of multimedia on cognitive aspects of decision-making. *International Journal of Accounting Information Systems* 10: 97-116.

Whitty, M. and S. Carville (2008). Would I Lie to You? Self-serving lies and other-oriented lies told across different media. *Computers in Human Behavior* 24: 1021-1031.

Wilks, T. and M. Zimbelman (2004a). Decomposition of Fraud-Risk Assessments and Auditors' Sensitivity to Fraud Cues. *Contemporary Accounting Research* 21(3): 719-745.

Wilks, T. and M. Zimbelman (2004b). Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud. *Accounting Horizons* 18(3): 173-184.

Zahra, S. , R. Priem and A. Rasheed (2005). The Antecedents and Consequences of Top Management Fraud. *Journal of Management* 31(6): 803-828.

Zellen, B. (2008). Document Fraud and Technology: A Double-Edged Sword. *Enterprise Innovator: Network & Information Security* January 15, 2008 [online] Available at http://enterpriseinnovator.com/index.php?articleID=14174&sectionID=25 (February 14, 2011).