Journal of Forensic and Investigative Accounting
LEARN MORE

Application of Underutilized Theories in Fraud Research: Suggestions for Future Research

*Kalana Malimage**

Introduction

Organizations are frequently exposed to different types of occupational fraud by their employees. These fraud incidents affect a wide range of people from management, employees, auditors, creditors, and investors. Businesses have been making efforts to reduce and prevent fraud and proactively manage fraud risk. Preventing fraud is a considerable challenge to organizations as fraudsters continuously discover different methods to commit fraud. The Association of Certified Fraud Examiners (ACFE) estimated that a total of $6.3 billion were lost due to fraud in 2016, where twenty-four percent of the cases caused losses of one million dollars or more (ACFE 2016). Detecting fraud is even more difficult as fraudsters usually attempt to conceal their tracks.

Businesses, therefore, should focus on identifying the factors that lead individuals to commit fraudulent acts. Fraud research, such as (Becker et al., 2006; Boyle et al., 2015; Dellaportas, 2013; Murphy and Free, 2016; Schuchter and Levi, 2013; Zakaria et al., 2016) have investigated factors that may influence individuals to commit fraud using different methodologies. These studies have provided important insights into why individuals perform deviant behaviors. All frauds have a common component: the intent to deceive for personal benefit. However, most of the research of fraud has been limited to the components of the fraud triangle (Cressey, 1953; Huber, 2016; Ramamoorti et al., 2013; Wells, 2005).

While the fraud triangle establishes a baseline to investigate factors influencing fraud, there could be many other variables that may influence an individual's intent to commit fraud.

There have been calls to move fraud research beyond the fraud triangle and the fraud diamond by conducting cross-disciplinary research that integrates established theories from sociology, psychology, and criminology (Ramamoorti, 2008; Trompeter et al., 2014). The purpose of this paper is to answer the call to extend fraud research beyond the fraud triangle by identifying three well-established and tested theories across different disciplines that apply to fraud research. These theories will assist fraud researchers in identifying antecedents of individual or organizational fraud behavior, extend and complement current findings conducted using the fraud triangle. In the next section of this paper, a review of the fraud triangle and its variants is conducted, as well as a review of recent field research related to the fraud triangle. Next, a review of three established theories from various disciplines are identified, and their applicability to fraud researchers are discussed along with suggestions for methodologies to use to test these theories. Finally, challenges that fraud researchers face are discussed with possible alternative approaches to face those challenges.

Fraud Triangle Theory and Fraud Diamond Theory

Fraud incidents in businesses have continued to increase at an alarming rate and employers have been trying to identify the factors behind why employees commit fraud (Cohen et al., 2010; Murphy and Dacin, 2011; Wells, 2001; Zawawi et al., 2008). Fraud researchers have also attempted to identify factors that lead individuals or corporations to commit fraud. The most established theories fraud researchers use is the Fraud Triangle Theory (FTT) (Cressey, 1953; Wells, 2005, 2011). Standards of auditing of fraud such as SAS No. 99 and ISA No. 240 have adopted the FTT. This theory is popular among researchers as it can be used to analyze fraud behavior in both individual and organizational levels. Fraud Diamond Theory (FDT) (Wolfe and Hermanson, 2004) extended the FTT by adding in a key component that was overlooked by the FTT.

The FTT and FDT attempt to identify elements that lead perpetrators to commit fraudulent acts. Enterprises spend a significant amount of time and effort to enforce internal controls to prevent and deter fraud. The FTT and FDT both capture psychological and causative factors of fraud occurrence. They identify those circumstances that propel or induce human behavior to fraud. In an organizational contest, weak internal controls, for example, will facilitate a mind that is already fraudulently disposed to commit fraud. However, it is more important to identify factors that lead employees to commit fraudulent acts, which can be used to install controls catered towards preventing and deterring those factors. The FTT consists of three components that are necessary for fraud to occur.

**The author is a professor at University of Wisconsin-Whitewater*

Perceived pressure, incentives or motive is the first component of FTT. The majority of the known fraud cases have involved some financial pressure on the perpetrator or simply because the perpetrator perceives pressure (Albrecht et al., 2008; Wells, 2011). Financial pressures may result from poor personal financial management, unemployment, and gambling habits. However, FTT and FDT do not limit pressure to just financial aspects, even though the ultimate destination of pressure, irrespective of the type, is money. Close to ninety-five percent of all fraud cases have been perpetrated due to financial pressures of the fraudster (Albrecht et al., 2008). Pressure by the employer to perform may also lead employees to commit fraudulent acts, as it was apparent in the recent fraudulent accounts creation at Wells Fargo (Sridharan and Hadley, 2018). Positive pressures can lead individuals to achieve goals. However, when goals are not attainable by normal means or are unrealistic, and career, compensation, and employment is at risk, individuals may resort to committing fraud to achieve those goals. Incentives such as bonuses or pay-related rewards, achieving sales targets, or price per share targets, may have numerous positive outcomes and encourage employees to work hard. However, in some situations, employment pressure from continuous compensation structures and financial interests of the management, are also likely to push employees towards deviant behaviors to achieve those goals (Sridharan and Hadley, 2018). While pressures and incentives may not be sufficient for fraudulent activity to occur, it motivates individuals to commit fraud.

Perceived opportunity is the second element in the FTT, which allows individuals to commit fraud due to inadequate internal controls and governance system. Organizations do not have control over their employees' personal financial pressures or their rationalization aspects, but they can ensure that there are no internal control weaknesses that can be exploited by the employees to commit fraud. Once an employee perceives that there is an opportunity to commit fraud such as lack of segregation of duties, weak internal controls and audits not being performed regularly, conditions are ripe for him or her to commit fraud. The perceptions are heightened when one of the other factors such as pressure/incentive and/or rationalization is present. It is also important to note that, similar to perceived pressure, opportunity is also a perception of the perpetrator (Wells, 2011). Several factors can increase the perceptions or the beliefs of a fraudster about opportunities to commit fraud. An employee may identify a lapse of controls in certain processes or lapse of segregation of duties and believe that he or she can commit fraud and not get caught. Similarly, an employee may see or know another colleague who commits fraud at the same workplace and continue to do so without being found. Another way the perceived opportunity may increase if there is a lack of disciplinary action for an employee who was caught guilty of committing fraud (Sauser, 2007). Kenyon and Tilton (2006) reflect similar positions about the increase in the fraudster's belief in opportunity due to lack of monitoring and supervision, weak internal controls, lack of an audit trail, and irregular job rotation.

Rationalization is the third component of the FTT, which refers to the justification of a fraudulent behavior as morally acceptable by the perpetrator. Researchers have defined rationalization differently. Rae and Subramaniam (2008) describe rationalization as a justification of deviant behavior by a fraudster who lacks personal integrity or moral reasoning. Lister (2007, p. 63), describes rationalization as "the oxygen that keeps the fire burning" and that the corporate culture may be a good indicator of the personal value systems of the employees. Rationalization is very important for a fraudster to carry out the deviant act such that if an act cannot be justified as ethical, the fraud would not be carried out (Dorminey et al., 2010; Jackson et al., 2010). The fraudster may rationalize these deviant actions using different justifications such as "I am only borrowing, and I will give it back," "My company can afford it,", "I did not get a raise, but I deserve one," and "Everyone else is doing it, so why shouldn't I?" (Ramamoorti, 2008; Zikmund, 2008). Individuals may use one or many of these reasons to justify their fraudulent behavior. Neutralization theory, which will be discussed in detail later, explains the different ways individuals may rationalize their fraudulent acts and how they can drift back and forth between being an ethical person to being a fraudster (Piquero et al., 2005).

When an individual can rationalize fraudulent behavior, a bridge is created between pressures/incentives and opportunity and the fraud triangle is created. Organizations must reduce opportunity with strong internal controls and enforcement while reducing perceptions of rationalization and pressure/incentives through training, awareness programs, and sanctions. The strength of each component and the context of the situation may moderate if and how fraud is committed and the extent of the fraud. This provides an opportunity for fraud researchers to identify how these components impact fraudulent behavior in different contexts (Howe and Malgwi, 2006).

FDT (Wolfe and Hermanson, 2004) adds a component of capability to the fraud triangle's existing components. Wolfe and Hermanson postulate that while the fraud triangle components of pressures/incentives, opportunity and rationalization may exist, it is unlikely that the fraudulent behavior will take place unless a fourth component is present: Capability. They describe that opportunity opens the doorway to fraud, pressures/incentives, and rationalization lead a person towards the

door and capability allows the fraudster to take advantage of the open doorway by walking through it, repeatedly. The capacity of a fraudster to commit a deviant act can be a combination of several traits and abilities. The first of such traits identified by Wolfe and Hermanson (2004) is the authoritative position or function within the organization. For example, a CEO or a CFO may have more influence or have system override capabilities than other employees, which increases the chances of them committing fraud. The second such trait is the skills and ability to commit the fraud. An employee with intelligence to exploit internal control weaknesses and understands how the system functions have a better chance of committing the deviant act. If a perpetrator does not have the skills and ability to commit fraud, he/she is unlikely to commit it. For example, an individual may have financial pressures at home, may have justified performing a fraudulent act and may have identified internal control weaknesses that may allow him to steal from the company. However, if he/she does not know how to perpetrate the fraud by exploiting system weaknesses, the fraud is unlikely to happen.

A third trait is personal ego and confidence that the fraud will not be detected. Therefore, egoistic individuals with high confidence are more likely to commit fraud. Finally, the fourth trait is the capability to deal with stress due to the risk of getting caught and manage the fraud over the long-term. A fraudster who wants to commit fraud over the long-term will have to constantly lie, hide and cover their tracks to make others believe there is no fraud taking place. This behavior is stressful, and only someone who can handle the stress can carry on with the deviant act. These personality traits in the newly introduced component of the fraud triangle provide the opportunity for researchers to investigate the fraud triangle along with different capabilities of individuals. Capability may be a moderator of the influences of the components of the fraud triangle on fraudulent behavior while directly influencing that behavior.

There have been many theoretical research articles published related to the FTT or the fraud triangle over the recent years. These theoretical articles have built on the fraud triangle framework and extended it further. As discussed previously, the fraud triangle was extended to a fraud diamond by Wolfe and Hermanson (2004) which added the capability component. A fraud square was introduced by Cieslewicz (2012), which called for the inclusion of the societal-level influences to the fraud triangle. Albrecht, Howe, and Romney (1984) created the "fraud scale" where personal characteristics and the occupational environment were combined. According to them, fraudulent acts are committed by individuals with personal characteristics of the fraud triangle with occupational pressure being heightened on a sliding scale. A model that includes the elements of Money, Ideology, Coercion, and Ego (MICE) was developed by Kranacher, Riley, Jr., and Wells (2011). The MICE model modifies the pressure and motivation components in the original fraud triangle. Dorminey et al., (2012), developed a meta-model that adds the probability of committing fraud such as the act, concealment, and conversion, to the components of the fraud triangle.

Empirical research studies that examine the FTT or its variations have been scant. The FTT also has been extended in different studies, but there have been very little follow-up of those with empirical evidence.

Murphy and Free (2016) conducted survey research among fraud perpetrators who were in prison, and auditors who investigated fraud and employees who have witnessed fraud within organizations. They investigated the existence of instrumental climate, which is define as a situation where employees make fraudulent decisions for their best interest or the organization's best interest. Their findings indicate that the instrumental climate was a key factor that was present when the fraud was perpetrated and suggests that future research take this important social dimension into account. Zakaria et al., (2016), investigated the internal control weaknesses and how it leads to fraudulent behavior in an oil and gas company. Using a mixed method approach that utilized document analysis and interviews, they found that internal control weaknesses were a major factor that lead to fraud. They also found that several employees colluded to commit fraud taking advantage of opportunities such as poor supervision and improper document control processes.

The study by Boyle et al., (2015) examined the fraud triangle, the fraud diamond, and CEO risk level among a sample of eighty-nine auditors in public accounting in a 2x2 experiment. Their results indicate that auditors who evaluated fraud risk factors based on the fraud diamond demonstrated higher fraud risk assessments than auditors who evaluated based on the fraud triangle. A study by Dellaportas (2013) examined the factors that influence accountants to commit fraud using the fraud triangle. The data were collected through face-to-face interviews of ten accountants serving sentences in prison for committing fraud and other offenses. While the findings differed from inmate to inmate, the overall findings suggest that the offenders used their position as accountants to deceive others when they faced a crisis. The findings also suggest that pressures varied from financial to non-financial and internal control deficiencies were taken advantage of by the perpetrators. The perpetrators also demonstrated various rationalizations for their fraudulent acts. Schuchter and Levi (2013) conducted face-to-face interviews with thirteen white-collar fraudsters in Switzerland and Austria, and they found that

perceived pressure was a salient factor in the fraudulent acts, while opportunity was not a critical element in white-collar crime.

Table I: Recent Empirical Research on FTT and its Variants

Publication	Sample	Methodology	Significant Findings
(Murphy and Free, 2016)	Prisoners, auditors, and employees who have witnessed fraud	Survey	Instrumental climate was found to be a key factor in fraud cases.
(Zakaria et al., 2016)	A single oil and gas company	Mixed method—document analysis and interviews	Internal control weaknesses the major contributing factor of fraud.
(Boyle et al., 2015)	Eighty-nine auditors	2x2 experiment	Fraud diamond provides better fraud risk assessments for auditors.
(Dellaportas, 2013)	Ten accountants who were serving sentences in prison for fraud	Face-to-face interview	Findings differed from inmate to inmate. Pressures varied from financial to non-financial. Opportunities were mostly control deficiencies and they demonstrated several rationalizations for their acts.
(Schuchter and Levi, 2013)	Thirteen white-collar fraudsters in Switzerland and Austria	Face-to-face interview	Perceived pressure salient to fraudster offenses. FTT elements highly influenced by corporate culture.
(Becker et al., 2006)	476 business students	Survey	Each FTT component was influential in student cheating behavior. Methods to reduce pressure, opportunities, and rationalization of students to cheat are discussed.

Their findings also suggest that a "fraud inhibiting inner voice" before the crime deterred individuals from committing fraud, but this voice gradually became quieter until the actual fraud occurred. The interviewees suggested that corporate culture in their workplace strongly influenced all the components of the fraud triangle that lead to the fraudulent act. A study conducted to explore academic dishonesty among 476 business students by Becker et al., (2006) found that each component in the fraud triangle was influential in student cheating behavior. They suggested a list of methods and recommendations to reduce pressure, opportunities, and rationalization to cheat. Table I lists a summary of the recent empirical studies discussed above involving the FTT or its extensions, the sample and methodology used for each of the study and their significant findings.

The FTT and its variants have been explored by fraud researchers many times. However, critics argue that the fraud triangle has been misused by fraud researchers (Huber, 2016). He argues that the original intention of Cressey (1953) was to explain theft or embezzlement and not to explain fraud. The use of terms fraud and embezzlement interchangeably by fraud researchers was criticized in that article. Donegan and Ganon (2008) also criticize the fraud triangle and related research due to the lack of solid empirical support, ignoring other factors that contribute to fraud and the one-dimensional analysis of the fraud perpetrators psychology. The fraud triangle has also been criticized due to assuming only individual acts and ignoring the group dynamics (Trompeter et al., 2013), ignoring the explanation of collusion and cultural differences (Cieslewicz, 2012), not adequately addressing every occurrence of fraud (Lokanan, 2015), fundamentally incomplete and biased translation from criminology to fraud examination (Morales et al., 2014), and not fully capturing the antecedents of fraud (Dorminey et al., 2012).

The fraud triangle is the most commonly used framework in fraud investigation and forensic accounting research and academia regardless of its critics (Huber, 2012; Smith and Crumbley, 2009). The research based on the FTT and its variants have increased the understanding of the motivations of fraudulent behavior. Trompeter et al., (2014) suggest that fraud researchers should move beyond the fraud triangle and examine findings of non-accounting research related to fraud and

forensics which would allow us to advance accounting research aimed at prevention, deterrence, and detection of fraud as well as informing the practice. They suggest exploring theories from non-accounting disciplines such as General strain theory (Merton, 1938), cognitive dissonance theory (Festinger, 1957), social identity theory, and game theory to advance fraud research to the next level. Ramamoorti (2008) suggests integrating behavioral sciences component into fraud by examining the psychology and sociology of fraud. He proposes the A-B-C model which allows the categorization of fraud as an individual (bad apple), collusive fraud (bad bushel), and the cultural and societal mechanisms that promotes fraud (bad crop). They later expanded their calls to apply psychology to prevent and detect financial fraud (Ramamoorti et al., 2013, 2014).

The rich theoretical foundations found in sociology, psychology, and criminology provide avenues for fraud researchers to conduct cross-disciplinary research (Trompeter et al., 2013, 2014) to gain better insights to the antecedents of fraud behavior. This article answers recent calls for integration of additional behavioral sciences content and theory from psychology, sociology, and criminology into the accounting curriculum as well as fraud research (Ramamoorti, 2008; Ramamoorti et al., 2013, 2014; Trompeter et al., 2014) by identifying three distinct theories from non-accounting disciplines that can be applied to expand fraud research beyond the fraud triangle.

Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB)

Theory of Reasoned Action (TRA), which was drawn from the social psychology discipline (Fishbein and Ajzen, 1975) is one of the most influential theories utilized in research on human behavior. The majority of the behavioral theories in use today are based on TRA, which has two core constructs: Attitude Toward Behavior and Subjective Norm. Attitude toward behavior has been defined as "an individual's positive or negative feelings (evaluative effect) about performing the target behavior" (Fishbein and Ajzen, 1975, p. 216). Subjective Norm refers to "the person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein and Ajzen, 1975, p.302). Both those constructs are hypothesized to influence behavioral intention to perform a certain behavior positively and the behavioral intention is posited to influence actual behavior positively. Due to its ability to predict any human behavior in applied settings, TRA has been used to predict many types of human behavior across many disciplines, for behaviors such as purchasing a certain product, using pills or birth controls, voting in the elections, going to church and using a certain technology (Sheppard et al., 1988). The TRA has been utilized in behavioral accounting research as well. For example, Law (2010), investigated accounting students' career choice in public accounting practices utilizing the TRA and found that attitude toward the behavior and subjective norms had a significant influence on the decision to select a CPA career.

The TRA was extended by Ajzen in 1991, by adding the construct of perceived behavioral control which was defined as "the perceived ease or difficulty of performing the behavior" (Ajzen, 1991, p.188). This new construct was based on the research findings that individuals' behavior is strongly influenced by how confident they are about their ability to perform it (Bandura, 1977). Perceived behavioral control is theorized to have a positive influence on behavioral intention to perform an act. It is also theorized to have a direct influence on the actual performance of the intended behavior.

The TRA was also used in studies investigating antecedents of unethical and fraudulent financial reporting in (Carpenter and Reimers, 2005; Zawawi et al., 2008), accountant whistleblower intentions (Brown et al., 2016), ethical decision making in the public accounting profession (Buchan, 2005), moral obligation in tax compliance (Bobek and Hatfield, 2003), predicting tax fraud (Yusof and Lai, 2014), corporate fraud (Awang et al., 2016; Cohen et al., 2010).

The TRA and TPB have become the basis of many behavioral theories across different disciplines. However, there has been much debate among researchers about the relationship between behavioral intention and actual performance of the behavior, as posited by TRA and TPB. Performance of behavior is considered a function of intentions and behavioral control as long as intentions and perceptions of controls assessed are related to the behavior of interest and that there are no intervening events that affect the intentions and control within the interval between assessment and observation of the behavior (Ajzen, 1991). Due to the difficulties in observing and measuring actual behavior, most researchers have simply used behavioral intention as a proxy for actual behavior (Warkentin et al., 2012). Some researchers have opted to collect self-reported actual behavior to circumvent this intention-behavior relationship (Crossler, 2010; Lee and Larsen, 2009; Liang and Xue, 2010; Woon et al., 2005). This intention-behavior gap has been examined extensively in meta-analysis studies, which have found inconsistent results (Sheeran, 2002; Sheeran et al., 2016; Sheppard et al., 1988; Sweeny and Moyer, 2015).

Theories from Various Disciplines

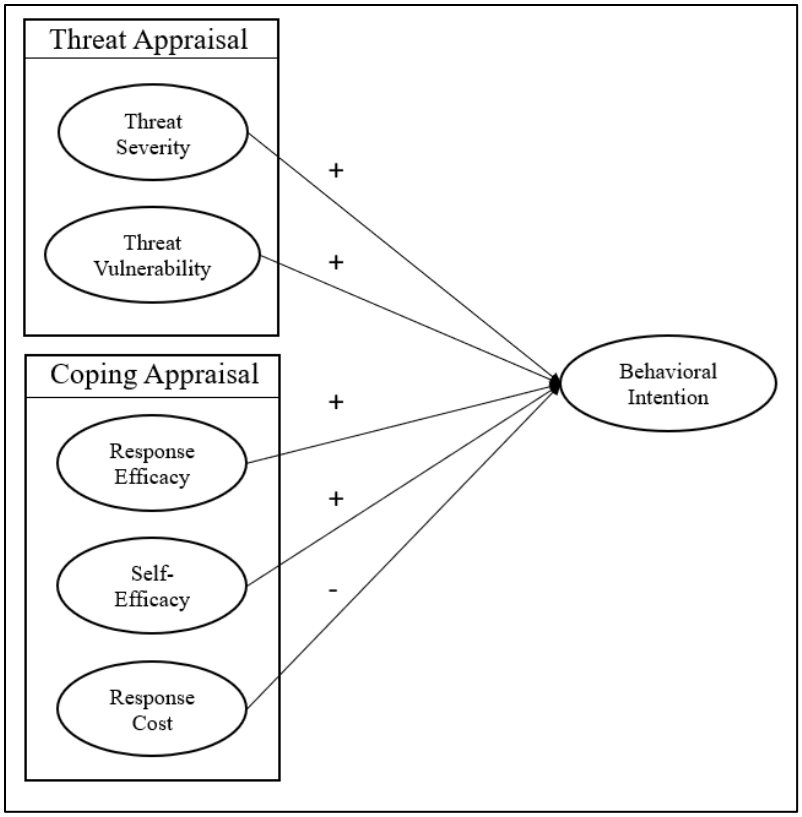
Protection Motivation Theory (PMT) (Fear Appeals and Others Around It)

Protection Motivation Theory (PMT) was originally developed by Rogers (1975) to demonstrate how fear appeals affect health attitudes and behaviors. Fear appeals are defined as "persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" (Witte et al., 1996, p. 329). The PMT consists of two main components which are part of a cognitive mediation process: Threat Appraisal and Coping Appraisal.

Threat appraisal consists of perceived threat vulnerability and perceived threat severity. The PMT suggests that once an individual receives information about a threat, a cognitive mediation process causes that individual to evaluate the threat. If the individual perceives that the threat is sufficiently severe and that he or she is susceptible to the threat, he or she will act to avoid or prevent the threat (Rogers, 1975). In addition to the cognitive appraisal of threat severity and threat susceptibility, individuals also form perceptions of the recommended response to the threat by assessing their own individual capabilities (self-efficacy), coupled with an assessment of the effectiveness of the response (response efficacy) (Bandura, 1977; Witte, 1992; Witte et al., 1996). Individuals also assess the cost related to performing a selected coping behavior (response cost). Response costs can be in the form of time, money and/or effort expended while performing the adaptive coping behavior (Floyd et al., 2000).

The perceptions created in the threat appraisal and coping appraisal processes will increase the likelihood of an individual performing a recommended response (Floyd et al., 2000). When the threat appraisal and coping appraisal processes are heightened, individuals are likely to become motivated to perform behaviors to protect themselves, other individuals, or organizations. (Floyd et al., 2000; Milne et al., 2000; Flynn et al., 1995; Beck and Feldman, 1983; Posey et al., 2013). However, response cost is posited to have a negative impact on behavioral intentions to perform a recommended response, precisely because an individual's capacity to react (respond) to or utilize a recommended response is a function of the response cost or his or her perception thereof.

Figure I: Protection Motivation Theory (PMT)



The PMT has been utilized heavily in management information systems research, especially in information security compliance. These research studies include contexts such as safe computing practices (Anderson and Agarwal, 2010); security policy compliance (Herath and Rao, 2009b; Woon et al., 2005); and information security (Johnston and Warkentin, 2010; Vance et al., 2012). Most of these studies have behavioral intention as a proxy for actual behavior since it is difficult to observe or capture actual behavior related to information security. Some studies, such as (Herath and Rao, 2009a; Johnston and Warkentin, 2010; Siponen and Vance, 2010; Vance et al., 2012) used self-reported behavior to proxy or model performance of the actual behavior. The conflicting findings in these studies, due chiefly to the threat variables, provide a valid empirical ground for further assessment and refinement of PMT.

Whereas PMT has been used in Management information systems studies, in has scarcely been applied in other business disciplines. Behavioral accounting research has rarely used it, except a recent study by Crossler et al., (2014) where they studied Bring Your Own Device (BYOD) policies among accounting students, non-accounting students and employees. Apart from Crossler et al., (2014), there appears to be no known published work linking PMT studies with fraud and forensic accounting. The concepts of fear and heightened threat appraisal, along with coping mechanisms to perform a certain behavior provide many opportunities to investigate this theoretical framework in an audit or fraud examination context. Future research can utilize PMT in several ways. First, PMT can be used to test the impact of anti-fraud training in corporations where the training can provide fear appeals (heightened threat severity and vulnerability) for possible fraud perpetrators, which will reduce intention to commit fraud. Second, PMT can be used to test managerial response to fraud by exploring the threat appraisal process for fraud by the management as well as the coping mechanisms that are applied to deal with the threat of fraud. Finally, PMT would allow fraud researchers to identify factors that may influence employees to report fraud (whistle-blowing).

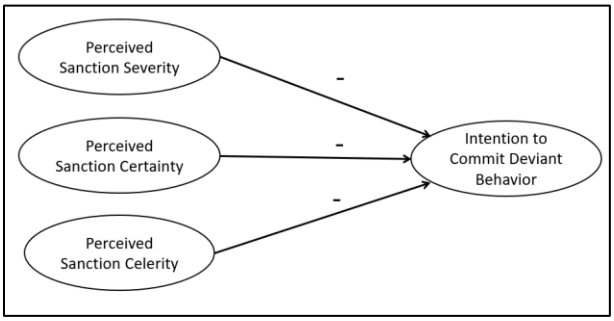
General Deterrence Theory (GDT)

The General Deterrence Theory (GDT) has some of its roots in Cesare Beccaria, who was a famous criminologist from Italy who lived in late eighteenth century (Monachesi, 1956). Beccaria argued against the death penalty as a punishment that is too severe. However, he argued that to deter crime, there should be a strong association between crime and punishment and that the pain of punishment should outweigh the illicit gains. He argued that rather than the severity of the punishment, it is its certainty and swift application that act as powerful deterrents.

The GDT is based on these three components, as deterrents to crime or deviant behavior and the premise that unwanted behavior can be deterred through the threat of punishment (Peace et al., 2003). The first component of GDT is perceived sanction severity which is the belief about the severity or magnitude of the sanctions that will be experienced because of unwanted behavior. However, according to Cesare Beccaria, a punishment that is too severe is unjust, and punishment that is not severe enough will not deter (Jacobs, 2010). Hence, there should be a reasonable balance between punishment and deterrence purpose. GDT suggests that when perceived sanction severity is high, it will decrease intentions to commit deviant behaviors.

The second component is perceived sanction certainty, which is a belief about the probability of apprehension and punishment for unwanted behavior (Tittle, 1980). It is hypothesized that when perceived sanction certainty is high, it will decrease intentions to commit deviant behavior. The third component is perceived sanction celerity, which is the belief about the swiftness of how the sanctions are applied after the apprehension for the commission of unwanted behavior (Gibbs, 1979). Therefore, it is hypothesized that when perceived sanction celerity is negatively correlated with the intention to commit deviant behavior. The conceptual model of GDT is shown in Figure II.

Figure II: General Deterrence Theory (GDT)



Many research studies (Bachman et al., 1992; Bates et al., 2017; Gibbs, 1975, 1979; Jacobs, 2010; Klepper and Nagin, 1989; Legge and Park, 1994) have been conducted in criminology about deviant or unwanted behavior, using GDT. However, the use of GDT in the business discipline is sparse. While there are many unwholesome behaviors by employees, encapsulated as fraud and abuse (Wells, 2011), the study of organizational fraud has proceeded as though there were no sanctions: the literature has been largely silent on the potential impact of sanctions on these abhorrent behaviors. Some research has been done in information security that investigated individuals' intention to engage in certain behavior such as security policy compliance and violation (Bulgurcu et al., 2010; D'Arcy and Herath, 2011; D'Arcy and Devaraj, 2012; Herath and Rao, 2009a, 2009b; Siponen and Vance, 2010) , information system (IS) misuse intention (D'Arcy et al., 2009; Hovav and D'Arcy, 2012), piracy intention (Peace et al., 2003). However, most of these studies did not examine sanction celerity, which is a main component of the GDT.

This perceived gap in fraud research provides fraud researchers an empirical opportunity to utilize GDT in several ways. First, fraud researchers and practitioners have been attempting to find ways to prevent, deter and detect fraud. However, there is a significant lapse in research and practice when it comes to the deterrence aspect of fraud. GDT provides the perfect opportunity to examine if sanctions such as termination of employment, demotion, the prospect of going to jail would deter individuals from committing fraud or intending to commit fraud. Second, this allows researchers to identify if a certain component of GDT (perceived severity, certainty, or celerity) has a higher impact on reducing the intention to commit fraud. Therefore, based on the findings, training and anti-fraud communication can be catered towards heightening the perception of one or more of the components. For example, if the research findings suggest perceived certainty has a significant impact, corporations can highlight the monitoring systems they have in place or demonstrate how easily previous fraudsters at the company were caught and prosecuted.

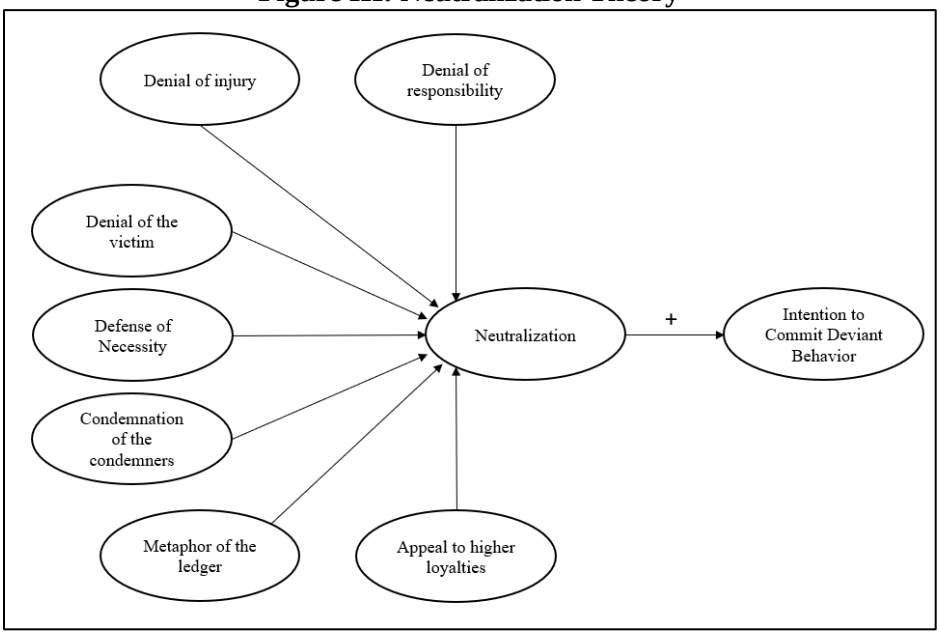
In addition to the three GDT components discussed above, three other potential explanatory factors in fraud research are self-control, moral belief, and employee position. Research suggests that individuals with low self-control are more likely to exhibit deviant behavior, such as fraud, as less likely to be concerned about the threat of sanctions, and are less concerned about the threat of sanctions (Pratt and Cullen, 2000). Another variable is moral belief, which is the extent to which one perceives a deviant or fraudulent activity to be morally offensive (Paternoster and Simpson, 1996). The third variable of interest is the employee position. Employees who are in different positions across the company (contract/permanent, full-time/part-time, managerial/administrative) are likely to respond differently to the threat of sanctions for deviant behavior (D'Arcy and Herath, 2011). These factors examined with GDT components will provide fraud researchers valuable insights into motivations of fraud and deterrence of fraud.

Neutralization Theory

Research in criminology argues that the impact of the threat of sanctions as explained by GDT may not be effective when employees use moral justifications to their fraud acts by using rationalization or neutralization techniques (Piquero et al., 2005). Rationalization, which is a component of the fraud triangle and its similarities with neutralization, has created some confusion and caused accounting researchers to use the terms interchangeably. It is no surprise that accounting researchers have not considered the differences between neutralization and rationalization, as research into the rationalization component of the fraud triangle has only recently received attention (Free, 2015). Neutralization is defined as the moral justification before the fraud is committed and rationalization is defined as the moral justification after the fraud is committed (Fritsche, 2005; Trompeter et al., 2013, 2014). It is important to consider the timing of the fraud justification when conducting research and applying it to anti-fraud programs (Trompeter et al., 2014).

Similar but distinct to the rationalization component of the fraud triangle, neutralization could potentially reduce the deterring impact of sanctions. Neutralization theory (Sykes and Matza, 1957) posits that individuals psychologically enable themselves to perform the deviant or rule-breaking behavior (such as fraud) by applying techniques of neutralization. For example, a fraudster may morally justify his or her fraudulent behavior by claiming that no harm is done to the company by their fraud, it will be just a one-time fraud, he/she deserved higher pay, etc. Sykes and Matza suggest that due to the neutralization of their behavior, individuals can move between being an ethical person and a fraudster (Piquero et al., 2005).

Figure III: Neutralization Theory



Sykes and Matza proposed five neutralization techniques that individuals may use: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners and appeal to higher loyalties. Two other techniques were added later: metaphor of the ledger (Klockars, 1974) and defense of necessity (Minor, 1981). Each of these techniques are described in Table II with examples.

Table II: Neutralization Techniques

Neutralization Technique	**Description**
Denial of responsibility	Individuals performing a deviant behavior rationalize that the behavior is out of his/her control. Example: "Did not know there was a policy that prevented such action". "The stated policy is unclear if a certain action is illegal or not".
Denial of injury	Justify a deviant behavior by minimizing the harm it causes. Example: "I am not stealing money, I am just borrowing". "My company is very large, so stealing just $1,000 will not harm it". "I stole from my company, it will not harm the employees".
Denial of the victim	Justify a deviant behavior by theorizing that the victim deserved the consequences. Example: "I have worked tirelessly for this company for many years and they did not give me a raise. Stealing money is fine because they deserve it".
Defense of necessity	Justify a deviant behavior that if the rule-breaking is viewed as necessary, one should not feel guilty about performing it. Example: "I am stealing from my company to pay my child's medical bills".
Condemnation of the condemners	Justify a deviant behavior by blaming those who are the target of the action. Example: "It is ok to violate company policies, because they are unreasonable".
Metaphor of the ledger	When an individual believes he/she has previously performed a number of good acts, they can afford to do some bad acts. Example: "I have never stolen before, so this one-time is justified".
Appeal to higher loyalties	Individuals who feel they are in a dilemma that must be resolved at the cost of a deviant behavior will use this technique. Example: "I have to violate company security policy by copying sensitive data to a USB drive to work from home, so I can meet the deadline".

Neutralization theory has been utilized in marketing (Rosenbaum et al., 2017; Harris and Dumas, 2009; Cromwell and Thurman, 2003), business ethics (De Bock and Van Kenhove, 2011; Chatzidakis et al., 2007), criminology (Maruna and Copes, 2005; Minor, 1981), and information security (Siponen and Vance, 2010; Siponen et al., 2014). It is surprising that neutralization has received scant attention from fraud researchers as it is directly related to the belief that fraudsters morally justify their deviant act. Neutralization theory is still very underutilized (Murphy and Dacin, 2011), especially in accounting and this gives researchers a perfect opportunity to explore it in the fraud context. Researchers can investigate only one or more of the neutralization techniques as it applies to their study and it is not necessary to test all the techniques in a single study (Fritsche, 2005). Fraud researchers can also investigate Neutralization Theory and GDT together to understand individual deviant behavior similar to Siponen and Vance (2010) or PMT and GDT together similar to (Herath and Rao, 2009a).

Fraud researchers have many avenues to extend their research beyond the fraud triangle by exploring non-accounting research that applies to fraud and deviant behavior. They may be able to complement the findings of prior research conducted related to the fraud triangle while taking into other factors such as personality, ego, values and other social factors that may impact fraud behavior. Theories such as Neutralization Theory and Cognitive Dissonance Theory can complement or extend findings of the rationalization component of the fraud triangle while theories such as PMT, GDT, TRA, and TPB can extend findings in the motive component. Finally, theories from psychology and sociology may provide opportunities to understand issues related to the opportunity component of the fraud triangle as well as social factors that may contribute to collusion in committing fraud. The PMT, GDT, Neutralization Theory, and other theories from non-accounting disciplines offer "validated scales, models, variables and constructs that when examined in the context of fraud and financially motivated crimes, might prove insightful to practice and research" (Trompeter et al., 2014, p.797).

Challenges for Fraud Research

Behavioral fraud researchers have employed various methodologies to investigate fraud in many different contexts. These methodologies range from surveys, interviews, and hypothetical scenarios to experiments. Due to the individuals' ethical context of behavioral fraud research, researchers face many challenges compared to behavioral research in other business disciplines. Due to the investigation of unethical. Deviant or fraudulent behavior, researchers are very likely to come across social desirability bias, especially when using self-reported instruments such as surveys or scripted face-to-face interviews.

One of the major challenges behavioral fraud researchers face is the response bias of respondents in their research sample. Among several response biases such as acquiescence bias, question order bias and demand characteristics, social desirability bias significantly impacts behavioral fraud researcher studies that contain self-reported research instruments. Social desirability bias influences an individual to answer a question in a survey or interview, in a way that makes him or her look more favorable to the researcher (Furnham, 1986; Nederhof, 1985). Some individuals tend to amplify good behavior while some will under-report deviant or negative behavior. For example, social desirability bias would influence the results of a study that investigates individuals' intentions to commit fraud. Societal view of individuals committing fraud is typically negative. Therefore, if the respondents are asked if they are likely to commit a certain fraud or if they intend to commit a certain fraud, they are very likely to state that they would not commit fraud to conform to the societal norm. This biased reporting of respondents can have detrimental effects on the validity of the self-reported research (Nederhof, 1985).

Another challenge fraud researchers face when conducting research is the difficulty to contriving an experimental setting that the institutional review board (IRB) would approve. Due to the sensitive nature of survey and interview questions that could be asked regarding individual perceptions of fraud, deviant behavior or criminal activity, IRB would be hesitant to approve most of the fraud research studies. There have been calls for more field research in a fraud context that involves interviews, surveys, and experiments with actual fraud perpetrators (Free, 2015). However, getting access to the subjects who may be incarcerated, privacy issues, self-serving biases, and ethics provide additional challenges to fraud researchers. These challenges make it difficult to test theories such as the ones discussed earlier with actual perpetrators.

One of the ways to circumvent respondent biases in fraud research is to use the hypothetical scenario method (Weber, 1992). This method uses vignettes or scenarios that "present subjects with written descriptions of realistic situations and then request responses on some rating scales that measure the dependent variables of interest" (Trevino, 1992, p 127–128). A meta-study of ethical decision-making articles found that fifty-five percent employed a scenario method as a method for assessing ethical/unethical behavior (O'Fallon and Butterfield, 2005; Pogarsky, 2004). Hypothetical scenario method provides several advantages to behavioral fraud researchers. First, scenarios provide an indirect way of measuring intention

to commit fraudulent behavior, by describing another's behavior in hypothetical terms. Therefore, the respondent may feel less intimidated to report his or her intention to commit a fraudulent act similarly to the person in the hypothetical scenario (Harrington, 1996). Second, scenarios provide a more realistic situation by incorporating contextual and situational details that would be important in decisions to commit a fraudulent act (Alexander and Becker, 1978; Klepper and Nagin, 1989). Third, this method provides a prospective measure of behavior by measuring intent to commit fraud, rather than past behavior (Bachman et al., 1992; Pogarsky, 2004).

Another method to reduce social desirability bias in self-reported instruments is to create an average of the participant responses whether the participant and others could commit fraudulent behavior. Using five or seven-point Likert-type scales ranging from "not likely" to extremely likely", the intention to commit fraud question can be presented as follows:

- What is the likelihood that you would do as (the person in the scenario) did, if you were in his/her position?
- What is the likelihood that others would do as (the person in the scenario) did, if others were in his/her position?

The first and third-person responses can be combined into an average response to be used as behavioral intention in the data analysis (Robinson et al., 2012).

In conclusion, there are many behavioral theories that are applicable to behavioral fraud research but have rarely been used. These theories can provide valuable insights into identifying antecedents of fraudulent behavior of individuals and possibly identify new variables that directly impact intention to commit fraud or moderate already established variables (Free, 2015; Ramamoorti, 2008; Trompeter et al., 2013, 2014). Using methods such as hypothetical scenario method and factorial survey methods, challenges such as social desirability bias can be reduced, and validity of the data can be increased. At a time where fraud incidents are constantly increasing, organizations would benefit greatly if researchers can find what influences employees to perceive certain emotions, intent to commit fraud and eventually commit the fraudulent behavior.

References

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Albrecht, W.S., Albrecht, C., and Albrecht, C.C. 2008. "Current Trends in Fraud and Its Detection: A Global Perspective," *Information Security Journal* (17).

Albrecht, W.S., Howe, K.R., and Romney, M.B. 1984. "Deterring Fraud: The Internal Auditor's Perspective," in *The Institute of Internal Auditors' Research Foundation*, Altamonte Springs, FL.

Alexander, C.S. and Becker, H.J. 1978. "The Use of Vignettes in Survey Research," *Public Opinion Quarterly* (42:1), pp. 93–104.

Association of Certified Fraud Examiners (ACFE). 2016. "Report to the Nation on Occupational Fraud and Abuse," Austin, TX.

Awang, Y., Ismail, S., Rahim, A., and Rahman, A. 2016. "Measuring the Potential for Financial Reporting Fraud in a Highly Regulated Industry," *The International Journal of Accounting and Business Society* (24:1), pp. 81–95.

Bachman, R., Paternoster, R., and Ward, S. 1992. "The Rationality of Sexual Offending: Testing a Deterrence/ Rational Choice Conception of Sexual Assault," *Law & Society Review* (26:2), pp. 343–372.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84), pp. 191–215.

Bates, L., Darvell, M.J., and Watson, B. 2017. "Young and Unaffected by Road Policing Strategies: Using Deterrence Theory to Explain Provisional Drivers' (Non)Compliance," *Australian & New Zealand Journal of Criminology* (50:1), SAGE PublicationsSage UK: London, England, pp. 23–38. (https://doi.org/10.1177/0004865815589824).

Beck, K.H. and Feldman, R.H. 1983. "Information Seeking among Safety and Health Managers," *The Journal of Psychology* (115:1), pp. 23–31.

Becker, D., Connolly, J., Lentz, P., and Morrison, J. 2006. "Using the Business Fraud Triangle to Predict Academic Dishonesty among Business Students," *Academy of Educational Leadership Journal* (10:1), pp. 37–54.

Bobek, D. and Hatfield, R. 2003. "An Investigation of the Theory of Planned Behavior and the Role of Moral Obligation in Tax Compliance," *Behavioral Research in Accounting* (15:1), pp. 13–28.

De Bock, T. and Van Kenhove, P. 2011. "Double Standards: The Role of Techniques of Neutralization," *Journal of Business Ethics* (99:2), pp. 283–296.

Boyle, D.M., DeZoort, F.T., and Hermanson, D.R. 2015. "The Effect of Alternative Fraud Model Use on Auditors' Fraud Risk Judgments," *Journal of Accounting and Public Policy* (34:6), Elsevier, pp. 578–596. (https://doi.org/10.1016/J.JACCPUBPOL.2015.05.006).

Brown, O., Hays, J., and Stuebs, M. 2016. "Modeling Accountant Whistleblowing Intentions: Applying the Theory of Planned Behavior and the Fraud Triangle," *Accounting and the Public Interest* (16:1), pp. 28–56.

Buchan, H.F. 2005. "Ethical Decision Making in the Public Accounting Profession: An Extension of Ajzen's Theory of Planned Behavior," *Journal of Business Ethics* (61:2), pp. 165–181.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523–548.

Carpenter, T.D. and Reimers, J.L. 2005. "Unethical and Fraudulent Financial Reporting: Applying the Theory of Planned Behavior," *Journal of Business Ethics* (60:2), pp. 115–129.

Chatzidakis, A., Hibbert, S., and Smith, A. 2007. "Why People Don't Take Their Concerns about Fair Trade to the Supermarket: The Role of Neutralisation," *Journal of Business Ethics* (74:1), pp. 89–100.

Cieslewicz, J.K. 2012. "The Fraud Model in International Contexts: A Call to Include Societal level Influences in the Model," *Journal of Forensic & Investigative Accounting* (4:1), pp. 214–254.

Cohen, J., Ding, Y., Lesage, C., and Stolowy, H. 2010. "Corporate Fraud and Managers' Behavior: Evidence from the Press," *Journal of Business Ethics* (95:2), pp. 271–315.

Cressey, D.R. 1953. *Other People's Money*, Montclair, NJ: Patterson Smith.

Cromwell, P.F. and Thurman, Q.C. 2003. "The Devil Made Me Do It: Use of Neutralizations by Shoplifters," *Deviant Behavior* (24:6), pp. 535–550.

Crossler, R.E. 2010. "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data," in *2010 43rd Hawaii International Conference on System Sciences*, IEEE, pp. 1–10. (https://doi.org/10.1109/HICSS.2010.311).

Crossler, R.E., Long, J.H., Loraas, T.M., and Trinkle, B.S. 2014. "Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention- Behavior Gap," *Journal of Information Systems* (28:1), pp. 209–226.

D'Arcy, J. and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091–1124.

D'Arcy, J. and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643–658.

D'Arcy, J. Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Perspective," *Information Systems Research* (20:1), pp. 79–98.

Dellaportas, S. 2013. "Conversations with Inmate Accountants: Motivation, Opportunity and the Fraud Triangle," *Accounting Forum* (37:1), pp. 29–39.

Donegan, J.J., and Ganon, M.W. 2008. "Strain, Differential Association, and Coercion: Insights from the Criminology Literature on Causes of Accountant's Misconduct," *Accounting and the Public Interest* (8:1), pp. 1–20.

Dorminey, J., Fleming, A., Kranacher, M., and Riley, R. 2010. "Beyond the Fraud Triangle," *The CPA Journal* (80:7), pp. 17–23.

Dorminey, J., Fleming, S., Kranacher, M., and Riley, R. 2012. "The Evolution of Fraud Theory," *Issues in Accounting Education* (27:2), pp. 555–579.

Fishbein, M. and Ajzen, I. 1975. *Belief, Attitude. Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley.

Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 39–50.

Flynn, M.F., Lyman, R.D., and Prentice-Dunn, S. 1995. "Protection Motivation Theory and Adherence to Medical Treatment Regimens for Muscular Dystrophy," *Journal of Social and Clinical Psychology* (14:1), pp. 61–75.

Free, C. 2015. "Looking through the Fraud Triangle: A Review and Call for New Directions," *Meditari Accountancy Research* (23:2), Emerald Group Publishing Limited , pp. 175–196. (https://doi.org/10.1108/MEDAR-02-2015-0009).

Fritsche, I. 2005. "Predicting Deviant Behavior by Neutralization: Myths and Findings," *Deviant Behavior* (26:5), Taylor & Francis Group , pp. 483–510. (https://doi.org/10.1080/016396290968489).

Furnham, A. 1986. "Response Bias, Social Desirability and Dissimulation," *Personality and Individual Differences* (7:3), pp. 385–400.

Gibbs, J. 1975. *Crime, Punishment, and Deterrence*, New York: Elsevier.

Gibbs, J. 1979. "Assessing the Deterrence Doctrine: A Challenge for the Social and Behavioral Sciences," *American Behavioral Scientist* (22:6), pp. 653–677.

Harrington, S.J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257–278.

Harris, L.C. and Dumas, A. 2009. "Online Consumer Misbehaviour: An Application of Neutralization Theory," *Marketing Theory* (9:4), pp. 349–402.

Herath, T. and Rao, R. 2009a. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106–125.

Herath, T. and Rao, R. 2009b. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154–165.

Hovav, A. and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information & Management* (20:1), pp. 79–98.

Howe, M.A. and Malgwi, C.A. 2006. "Playing the Ponies: A $5 Million Embezzlement Case," *Journal of Education for Business* (82:1), pp. 27–33.

Huber, W.D. 2012. "Is Forensic Accounting in the United States Becoming a Profession?," *Journal of Forensic and Investigative Accounting* (4:1), pp. 255–284.

Huber, W.D. 2016. "Forensic Accounting, Fraud Theory, and the End of the Fraud Triangle," *Journal of Theoretical Accounting Research* (12:2), pp. 28–48.

Jackson, K., Holland, D., Albrecht, C., and Woolstenhulme, D. 2010. "Fraud Isn't Just for Big Business: Understanding the Drivers, Consequences, and Prevention of Fraud in Small Business," *Journal of International Management Studies* (5:1), pp. 160–164.

Jacobs, B. 2010. "Deterrence and Deterrability," *Criminology* (48:2), pp. 417–441.

Johnston, A.C. and Warkentin, M.E. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:2), pp. 549–566.

Kenyon, W.,and Tilton, P.D. 2006. *Potential Red Flags and Fraud Detection Techniques: A Guide to Forensic Accounting Investigation*, (First Edit.), New Jersy: John Wiley & Sons Inc.

Klepper, S. and Nagin, D. 1989. "The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited," *Criminology* (27:4), pp. 721–746.

Klockars, C.B. 1974. *The Professional Fence*, Free Press.

Kranacher, M.J., Riley, Jr., R.A., and Wells, J.T. 2011. *Forensic Accounting and Fraud Examination*, New York: John Wiley & Sons Inc.

Law, P.K. 2010. "A Theory of Reasoned Action Model of Accounting Students' Career Choice in Public Accounting Practices in the Post-Enron," *Journal of Applied Accounting Research* (11:1), pp. 58–73.

Lee, Y. and Larsen, K.R. 2009. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18), pp. 177–187. (https://doi.org/10.1057/ejis.2009.11).

Legge, J. and Park, J. 1994. "Policies to Reduce Alcohol-Impaired Driving: Evaluating Elements of Deterrence," *Social Science Quarterly* (75:3), pp. 594–606.

Liang, H. and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective* Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (Vol. 11). (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.170.5816&rep=rep1&type=pdf).

Lister, L.M. 2007. "A Practical Approach to Fraud Risk," *Internal Auditor*, pp. 1–30.

Lokanan, M.E. 2015. "Challenges to the Fraud Triangle: Questions on Its Usefulness," *Accounting Forum* (39:3), pp. 201–224.

Maruna, S. and Copes, H. 2005. "What Have We Learned from Five Decades of Neutralization Research?," *Crime and Justice* (32:221), pp. 221–320.

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), pp. 106–143.

Minor, W.W. 1981. "Techniques of Neutralization: A Reconceptualization and Empirical Examination," *Journal of Research in Crime and Delinquency* (18:2), pp. 295–318.

Monachesi, E. 1956. "Pioneers in Criminology IX--Cesare Beccaria (1738-1794)," *Journal of Criminal Law and Criminology* (46:4), pp. 439–449.

Morales, J., Gendron, Y., and Guénin-Paracini, H. 2014. "The Construction of the Risky Individual and Vigilant Organization: A Genealogy of the Fraud Triangle," *Accounting, Organizations and Society* (39:3), pp. 170–194.

Murphy, P.R. and Dacin, T.M. 2011. "Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations," *Journal of Business Ethics* (101:4), pp. 601–618.

Murphy, P.R. and Free, C. 2016. "Broadening the Fraud Triangle: Instrumental Climate and Fraud," *Behavioral Research in Accounting* (28:1), pp. 41–56.

Nederhof, A. J. 1985. "Methods of Coping with Social Desirability Bias: A Review," *European Journal of Social Psychology* (15:3), pp. 263–280.

O'Fallon, M. and Butterfield, K. 2005. "A Review of the Empirical Ethical Decision-Making Literature: 1996–2003," *Journal of Business Ethics* (59:4), pp. 375–413.

Paternoster, R. and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Soceity Review* (30:3), pp. 549–584.

Peace, A.G., Galletta, D., and Thong, J. 2003. "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp. 153–177.

Piquero, N.L., Tibbetts, S.G., and Blankenship, M.B. 2005. "Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime," *Deviant Behavior* (26:2), pp. 159–188.

Pogarsky, G. 2004. "Projected Offending and Implications for Heterotypic Continuity," *Criminology* (42:1), pp. 111–135.

Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R J., and Courtney, J.F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189–1210.

Pratt, T.C., and Cullen, F.T. 2000. "The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis," *Criminology* (38), pp. 931–964.

Rae, K. and Subramaniam, N. 2008. "Quality of Internal Control Procedures: Antecedents and Moderating Effect on Organisational Justice and Employee Fraud," *Managerial Auditing Journal* (23:2), pp. 104–124.

Ramamoorti, S. 2008. "The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component into Fraud and Forensic Accounting Curricula," *Issues in Accounting Education* (23:4), pp. 521–533.

Ramamoorti, S., Morrison, D., and Koletar, J.W. 2014. "Bringing Freud to Fraud," *Journal of Forensic & Investigative Accounting* (6:1), pp. 47–81.

Ramamoorti, S., Morrison, D., Koletar, J.W., and Pope, K. R. 2013. *A.B.C.'s of Behavioral Forensics: Applied Psychology to Financial Fraud Prevention and Detection*, Hoboken, NJ: John Wiley & Sons.

Robinson, S.N., Robertson, J.C., and Curtis, M.B. 2012. "No Title," *Journal of Business Ethics* (106), pp. 213–227.

Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91:1), pp. 93–114.

Rosenbaum, M.S., Kuntze, R., and Ross-Wooldridge, B. 2017. "Understanding Why Customers Choos to Abuse or Not to Abuse, Return Policies: The Customer'S Return Is Not Always Legitimate!," in *Proceedings of the Academy of Marketing Science*, C. C.L. (ed.), Springer, Cham.

Sauser, W.I. 2007. "Employee Theft: Who, How, Why, and What Can Be Done," *Advanced Management Journal* (72:3), pp. 13–25.

Schuchter, A. and Levi, M. 2013. "The Fraud Triangle Revisited," *Security Journal*.

Sheeran, P. 2002. "Intention—Behavior Relations: A Conceptual and Empirical Review," *European Review of Social Psychology* (12:1), pp. 1–36.

Sheeran, P., Webb, T.L., and TL. 2016. "The Intention–Behavior Gap," *Social and Personality Psychology Compass* (10:9), pp. 503–518. (https://doi.org/10.1111/spc3.12265).

Sheppard, B.H., Hartwick, J., and Warshaw, P.R. 1988. "The Theory of Reasoned Action: A Meta- Analysis of Past Research with Recommendations for Modifications and Future Research," *Journal of Consumer Research* (15:3), pp. 325–343.

Siponen, M., Mahmood, M.A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), p. 217.

Siponen, M. and Vance, A. 2010. "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487–502.

Smith, G. and Crumbley, D. 2009. "How Divergent Are Pedagogical Views toward the Fraud/ Forensic Accounting Curriculum?," *Global Perspectives on Accounting Education* (6:1), pp. 1–24.

Sridharan, U. and Hadley, L. 2018. "Internal Audit, Fraud and Risk Management at Wells Fargo," *Journal of the Academic Business World* (12:1), pp. 49–53.

Sweeny, A.M. and Moyer, A. 2015. "Self-Affirmation and Responses to Health Messages: A Meta-Analysis on Intentions and Behavior," *Health Psychology* (34:2), pp. 149–159.

Sykes, G. and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review* (22:6), pp. 664–670.

Tittle, C. 1980. *Sanctions and Social Deviance: The Question of Deterrence*, New York: Praeger.

Trevino, L.K. 1992. "Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:2), pp. 121–136.

Trompeter, G., Carpenter, T., Desai, N., Jones, K., and Riley, D. 2013. "Asynthesis of Fraud Related Research," *Auditing: A Journal of Practice and Theory* (32:1), pp. 769–804.

Trompeter, G., Carpenter, T., Jones, K., and Riley, D. 2014. "Insights for Research and Practice: What We Learn about Fraud from Other Disciplines," *Accounting Horizons* (28:4), pp. 769–804.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3), pp. 190–198.

Warkentin, M., Straub, D., and Malimage, K. 2012. "Featured Talk: Measuring Secure Behavior: A Research Commentary," *Annual Symposium on Information Assurance*, Albany, NY. (https://www.albany.edu/iasymposium/proceedings/2012/5-Warkentin_Straub&Malimage.pdf).

Weber, J. 1992. "Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations," *Business Ethics Quarterly* (2:2), pp. 137–160.

Wells, J.T. 2001. "Why Employees Commit Fraud," *Journal of Accountancy*.

Wells, J.T. 2005. *Principles of Fraud Examination*, Hoboken, N.J.: John Wiley & Sons Inc.

Wells, J.T. 2011. *Corporate Fraud Handbook: Prevention and Detection*, Hoboken, New Jersey: John Wiley & Sons Inc.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59), pp. 329–349.

Witte, K., Cameron, K.A., McKeon, J.K., and Berkowitz, J.M. 1996. "Predicting Risk Behaviors: Development and

Validation of a Diagnostic Scale," *Journal of Health Communication* (1), pp. 317–341.

Wolfe, D. and Hermanson, D.R. 2004. "The Fraud Diamond: Considering Four Elements of Fraud.," *The CPA Journal* (74:12), pp. 38–42.

Woon, I.M.Y., Low, R.T., and Tan, G.W. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the 26th International Conference on Information Systems,* Las Vegas, NV, pp. 367–380.

Yusof, N.A.M. and Lai, M.L. 2014. "An Integrative Model in Predicting Corporate Tax Fraud," *Journal of Financial Crime* (21:4), pp. 424–432.

Zakaria, K.M., Nawawi, A., and Salin, A.S.A. P. 2016. "Internal Controls and Fraud – Empirical Evidence from Oil and Gas Company," *Journal of Financial Crime* (23:4), pp. 1154–1168. (https://doi.org/10.1108/JFC-04-2016-0021).

Zawawi, S., Jusoff, K., Abdul Rahman, R., and Idris, K. 2008. "Behavioural Intention for Fraudulent Reporting Behaviour Using Cognitive Theory," *Asian Social Science* (4:7).

Zikmund, P.E. 2008. "Reducing the Expectation Gap," *The CPA JournalCPA* (78:6), pp. 20–25.