ISSUES IN ACCOUNTING EDUCATION
Vol. 27, No. 2
2012
pp. 555–579

American Accounting Association
DOI: 10.2308/iace-50131

The Evolution of Fraud Theory

Jack Dorminey, A. Scott Fleming, Mary-Jo Kranacher, and Richard A. Riley, Jr.

ABSTRACT: This paper revisits the Fraud Triangle, highlighting recent findings and contemporary thinking in the anti-fraud community to develop a meta-model of fraud for use in accounting instruction and research. The importance of the Fraud Triangle is particularly important as a model for assessing the risk of fraud, but it is only one component of an overall audit risk assessment plan. Explicit reference to the auditor's responsibility in identifying the risks of material misstatement arising from fraud is included in the guidance provided by both the AICPA and PCAOB (2010). Identifying fraud risk is a significant element of assurance services, and necessitates a model reflecting the current thinking surrounding the fraud event. To enhance our understanding of the fraudster's motivations and improve the anti-fraud community's ability to prevent, deter, detect, investigate, and remediate fraud, researchers and practitioners have offered insights beyond the Fraud Triangle. These insights are summarized in this manuscript and presented in a meta-model, providing a foundational resource for educators and researchers pursuing the study of fraud. Key aspects of the meta-model include instructional benefits in the classroom and an empirical approach from a research standpoint.

Keywords: fraud; fraudster; predator; risk assessment; Fraud Triangle; fraud diamond; fraud pentagon; accidental fraudster; predatory fraudster; management override; collusion; white-collar crime.

INTRODUCTION

This paper provides an instructional resource in the form of a meta-model for the discussion of white-collar crime and fraud theories in the classroom and to assist future fraud research.[1] We begin the discussion with a review of foundational theory that attempts to explain financially motivated crime, move to the well-known Fraud Triangle, and then discuss

Jack Dorminey is an Assistant Professor and A. Scott Fleming is an Assistant Professor, both at West Virginia University, Mary-Jo Kranacher is a Professor at York College–CUNY, and Richard A. Riley, Jr. is a Professor at West Virginia University.

We thank Barbara Apostolou, Sridhar Ramamoorti, and the editors and reviewers of the journal for their interest in this research and making suggestions that have significantly improved this manuscript, both in substance as well as style.

Supplemental materials can be accessed by clicking the link in Appendix A.

Published Online: January 2012

[1] A series of PowerPoint slides are available (see Appendix A). The PowerPoint presentation provides a summary of the material discussed herein in graphical format, which should support the effective transfer of concepts and knowledge from instructor to students.

additional constructs that attempt to explain conditions and motivations of fraudsters, beyond the Fraud Triangle. Through a meta-model, we unify many of the existing theories on fraud in a manner that helps explain the characteristics of white-collar criminals in a more comprehensive manner. Additionally, from the context of our meta-model, we attempt to identify potential areas for further research.

This paper fills a gap in the accounting education literature in multiple ways. First, we provide a comprehensive discussion of the various antecedents to fraud and financial crime, including the Fraud Triangle and significant work that has followed. Cressey's (1950, 1953) work on trust violation was seminal in nature, yet represented only the first of many steps toward developing our understanding of white-collar crime. Later insights, such as the Fraud Scale (Albrecht et al. 1984) and the Fraud Diamond (Wolfe and Hermanson 2004), incrementally add to our understanding of fraud. Secondly, we provide a cohesive framework in the form of a meta-model from which to teach, relate, and explore fraud theory. Third, building from Ramamoorti (2008), we discuss potential gaps in the research that may require an interdisciplinary approach, particularly given the behavioral aspects and nature of fraud. Last, we believe there is a need for continued discussion in instruction and research on white-collar crime, given the continuation of illegal acts and the great economic cost.[2]

The paper proceeds in the following manner: We begin with an overview of fraud, the foundations of fraud theory, and a simple model of fraud, followed by the well-known Fraud Triangle and the Triangle of Fraud Action. We then expand upon the characteristics of the perpetrator with the various theories of fraud that have been developed over time, and use a meta-model to illustrate possible structural links. Finally, we discuss future research potential and gaps in existing research.

Early Fraud

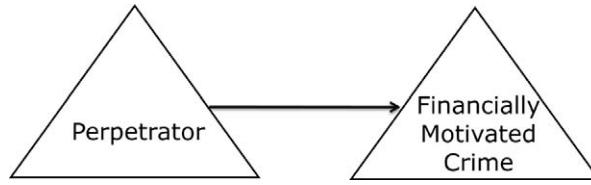
Financial crime and fraud have probably existed since the beginning of commerce. Woodward et al. (2003) noted the use of rudimentary biometrics thousands of years ago as a means of identifying trusted traders—the inference being that untrustworthy market participants have existed since man began to trade. Keay (1992), Robins (2007), and others report on what may be the first public company financial statement fraud at the British East India Company in the late 1600s. Adam Smith (1776) recognized the shortcomings of the modern corporation including the erosion of shareholder value due to waste from fraud and abuse.

With this in mind, we posit a basic fraud model in Figure 1. This model highlights the separation of the individual who perpetrates the crime from the criminal act.

Over the last 60 years, more sophisticated theories have been developed which differentiate fraud and its motivations from other forms of financially motivated crimes, such as theft and burglary. Each of these fraud theories provides a unique perspective of fraud as well as insight into the mind of the fraudster. The evolution of these theories has, therefore, moved the current view of fraud far beyond the simplicity of Figure 1. Research into these models identifies: constructs and characteristics that describe the individual committing the crime; mediators and moderators of the vector between the perpetrator and crime, such as accounting controls and risk assessment; and actions that deconstruct the particulars of the crime into identifiable functions. It is from this basic conceptual model that we begin to build on our understanding of fraud and white-collar crime.

[2] The Association of Certified Fraud Examiners (ACFE), in its 2010 Report to the Nations on Occupational Fraud & Abuse, estimates that the annual cost of fraud approaches 5 percent of revenues for a typical firm and may be as large as $2.9 trillion dollars worldwide (ACFE 2010).

FIGURE 1
Basic Conceptual Model for Financially Motivated Crime



White-Collar versus Other Crime—Foundations of Fraud Theory

Edwin H. Sutherland (1940) is credited with the term "white-collar crime." While earlier criminologists and sociologists examined the broad topic of crime, focusing mainly on street and violent crime, Sutherland was the first to integrate crimes of the upper white-collar class with economics and business activity. In the context of overt lawbreaking by many of the nineteenth-century robber barons, Sutherland describes the white-collar criminal as the suave professional who principally violates "delegated or implied trust."[3] Sutherland notes that prior theories of criminality tend to describe poverty as a primary driver of crime, but poverty is seldom central to white-collar crime.

Sutherland (1940, 1944) differentiates white-collar criminals from street or violent criminals in three major ways. First, he argues that the status of a professional within society creates an atmosphere of both admiration and intimidation. Members of society admire the professional, but are also afraid of retribution if they antagonize such individuals. Admiration and fear lead to lesser punishments for white-collar criminals.

Second, because of the status of the professional, there is less reliance on the traditional criminal justice system, and lesser penalties are typically applied (e.g., civil actions of the SEC). Until recently, civil actions, injunctions, fines, or probation were often prescribed for fraudulent offenses, with any notation of a "criminal" act omitted from the adjudication proceedings.

Third, white-collar crimes are less obvious than violent crimes for several reasons: the consequences borne by the public may be diffused over a longer period, the act may be spread among more individuals, and the victims may be more difficult to identify and not well organized. Citing societal tolerance and lesser punitive measures for white-collar crimes, Sutherland (1940, 1944) asserted that the legal regime of the time was ineffective.[4]

The Fraud Triangle

During this period, Sutherland was mentoring Donald R. Cressey, a student working on his Ph.D. in criminology, who began research on embezzlement behavior. From interviews with inmates in the Illinois State Penitentiary at Joliet, Cressey noticed common characteristics among convicts serving time for white-collar offenses. Based on his observations, Cressey (1950, 1953) hypothesized three criteria for criminal violations of trust: (1) a non-shareable financial problem; (2)

[3] Readers may note that this "delegated or implied trust" has ties to agency theory where the principal or shareholder hires agents, or management, to act on their behalf (Berle and Means 1932; Jensen and Meckling 1976).

[4] Snider (1982) is consistent with the argument that white-collar criminals are punished less severely than traditional criminals, but Braithwaite (1985) contends that attitudes toward white-collar crime are becoming increasingly punitive.

knowledge of the workings of a specific enterprise and the opportunity to violate a position of trust; and (3) the ability to adjust one's self-perception such that violating this trust does not constitute, in his or her mind, criminal behavior. Cressey (1950, 1953) hypothesized that for fraud to occur, each of the three criteria must be present: perceived pressure, perceived opportunity, and rationalization. One representation of his theory, illustrated in Figure 2, eventually evolved into what we know today as the "Fraud Triangle."

Perceived *pressure* from a non-shareable financial problem creates the motive for the crime. An individual may deem an issue non-sharable due to his/her perception of the social stigma associated with owning such a problem. Additionally, a strong sense of ego or pride may prevent an individual from seeking help or sharing the problem.

Perceived *opportunity* is the perception (1) that a control weakness is present, and importantly, (2) that the likelihood of being caught is remote. Therefore, perceived opportunity requires the ability to commit the act, and to do so without detection.

Rationalization is an attempt to reduce the cognitive dissonance within the individual (Festinger 1957; Ramamoorti 2008; Ramamoorti et al. 2009). Cressey (1950, 1953) observed that individuals who commit fraud desire to remain within their moral comfort zone. Therefore, at least internally, the fraudster seeks to justify the fraudulent action *before* the first fraud act. Cressey (1950, 1953) noted that the fraud perpetrator does not want to be considered a trust violator, but rather considers his/her dilemma as a special exception, a situation that allows them not to view themselves in a negative manner. The inconsistency of thought, "what is right" versus "what I am about to do," for first-time perpetrators must be reconciled. Only through rationalization is the perpetrator able to reduce the dissonance and proceed without compunction.

Cressey's rationalization characteristic is consistent with Hollinger and Clark's (1983) conclusion that employees steal primarily as a result of poor workplace conditions. Employees find it easier to rationalize their theft as compensation for putting up with unfavorable working conditions. Simply, the employees rationalize stealing by convincing themselves that "they owe me." Hollinger and Clark (1983) posited the following relationships:

1. There is little correlation between personal income levels and fraud. Income does not appear to be a predictor of theft; employees at all income levels commit fraud.
2. There is a positive correlation between job dissatisfaction and employee deviance, including fraud.
3. There is a negative correlation between controls and incidences of employee deviance.

Cressey's (1950, 1953) fundamental observation is that with a non-sharable financial challenge, a perceived opportunity to steal with little fear of detection, and a morally defensible excuse, an otherwise upstanding and professional individual may commit fraud. The Fraud Triangle

FIGURE 2
The Fraud Triangle

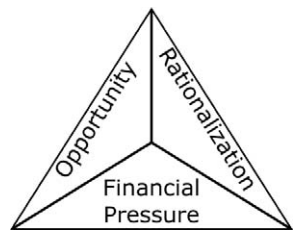
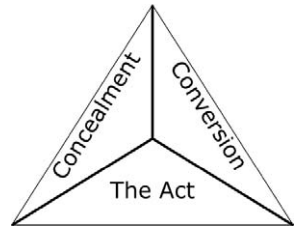


FIGURE 3
Triangle of Fraud Action: The Crime



was developed based on these three fundamental observations, and it forms the basis for most discussions of white-collar crime in accounting curricula.

The Triangle of Fraud Action

In addition to an examination of the theories centered on the white-collar criminal (the actor), we extend our discussion to include the characteristics of the white-collar crime (the action). A corollary to the Fraud Triangle is the lesser-known Triangle of Fraud Action, sometimes referred to as the *Elements of Fraud* (Albrecht et al. 2006; Kranacher et al. 2011). While the Fraud Triangle identifies the conditions under which fraud may occur, the Triangle of Fraud Action describes the actions an individual must perform to perpetrate the fraud (Figure 3).

The three components of the Triangle of Fraud Action are the *act*, *concealment*, and *conversion*. The *act* represents the execution and methodology of the fraud, such as embezzlement, check kiting, or material fraudulent financial reporting. *Concealment* represents hiding the fraud act; examples of concealment include creating false journal entries, falsifying bank reconciliations, or destroying files. *Conversion* is the process of turning the ill-gotten gains into something usable by the perpetrator in a way that appears to be legitimate; examples include laundered money, cars, or homes. The incremental value of the Triangle of Fraud Action is that it represents specific actions that can be documented with evidence, as well as control points where the fraud or potential fraud may be prevented, detected, or remediated. That is, anti-fraud professionals may develop certain measures, controls, or structure their audits to illuminate the act, the concealment, or the conversion.

The Triangle of Fraud Action is valuable to the investigator where proof of intent is required. While the Fraud Triangle points investigators to *why* people might commit fraud, the evidentiary trail might be weak or nonexistent. For example, the financial pressure and rationalization elements of the Fraud Triangle are not directly observable. Accordingly, a lack of fraud evidence is not proof that a fraud has not occurred (Ramamoorti 2008). Therefore, anti-fraud professionals need an evidenced-based approach to conduct investigations. The Triangle of Fraud Action is helpful in this regard because the elements can be directly observed and documented. The Triangle of Fraud Action, therefore, represents a model for detecting white-collar crimes and obtaining prosecutorial evidence. Evidence of the act, concealment, and conversion can be collected and presented during adjudication. Further, when considered in total, the Triangle of Fraud Action makes it difficult for the perpetrator to argue that the act was accidental or to deny his/her role in the act. Evidence of concealment, in particular, provides a compelling argument that the act was intentional.

BEYOND THE FRAUD TRIANGLE

The Fraud Triangle provides an efficient conceptual model that has broadly served as an aid to the anti-fraud community in understanding the antecedents to fraud. For example, the ACFE (2009)

Fraud Examiners Manual and virtually every auditing and information systems textbook covers the Fraud Triangle. Further, elements of the Fraud Triangle are an integral part of the PCAOB's AU Section 316, *Consideration of Fraud in a Financial Statement Audit*(AICPA 2002a),[5] and the AICPA's redrafted Statement on Auditing Standards (SAS), *Consideration of Fraud in a Financial Statement Audit*.[6] In addition, research in the area provides support for the existence of Fraud Triangle conditions within companies where fraud schemes have been perpetrated (Bell and Carcello 2000; Hogan et al. 2008). As a recent example, LaSalle (2007) shows that the use of the Fraud Triangle can lead to improved risk assessment.

Nonetheless, financial markets and white-collar schemes have only grown in complexity and in creativity since Sutherland reported his observations in 1940.[7] Further, a careful evaluation of certain fraudulent acts demonstrates that the Fraud Triangle may not fully capture the antecedents to fraud. For example, commercial bribery requires more than one person; although possible, it is doubtful that every party to a bribery scheme is motivated by a non-sharable financial need as described by the Fraud Triangle. In this context, the Fraud Triangle does not appear to adequately address all the attributes of the white-collar criminal for these types of acts.

Several models and extended theories of fraud attempt to explain why individuals commit fraud and financial crimes beyond the rationale afforded by the Fraud Triangle. These additional models seek to identify supplementary psychological or sociological antecedents (personality and behavioral characteristics) to describe those tending toward fraud. In Figure 4 we posit the first step in building our meta-model of white-collar crime.

At this initial step we relate the Fraud Triangle to the Triangle of Fraud Action and identify an area around the Fraud Triangle where other theories and models are informative. The area around the Fraud Triangle, *Individual Characteristics—Measures, Constructs, and Combinations of Hazard*, is where we introduce additional behavior and decision models that affect rationalization, perceived opportunity, and financial pressure. Models in this area include the Fraud Scale, M.I.C.E., the predator versus the accidental fraudster, the Fraud Diamond, and the A-B-C analysis of white-collar crime. The area contained within the box of the model represents the entry point for the additional constructs afforded by these models. We emphasize in particular the psychological and sociological constructs as critical elements for future fraud research. This part of our model is instructional in that many interdisciplinary constructs have overlapping characteristics that explain the perpetrator. That is, the relevant constructs are likely not mutually exclusive. The additional theories build upon the Fraud Triangle in a manner beneficial to the instructor, the researcher, and the practitioner alike, providing greater insight into possible criteria and motivations from which fraud may be sparked. The line between the perpetrator and the crime represents the probability vector, upon which many factors mediate or moderate the likelihood of fraud.

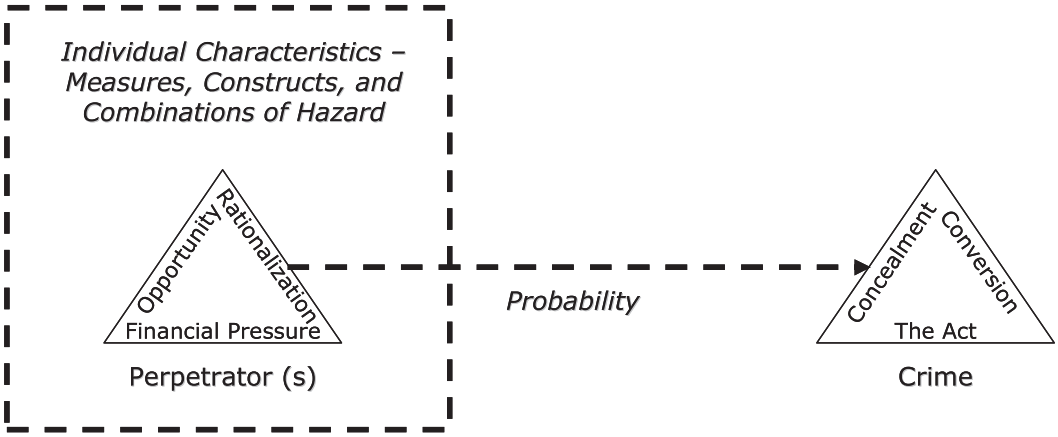
---

[5] PCAOB is responsible for issuing auditing standards for issuing firms. Reference to assessing and responding to the risk of fraud is included throughout the Auditing Standards issued by PCAOB and is codified in PCAOB's AU 316.

[6] As part of the Auditing Standards Board (ASB) Clarity Project, ASB is converging U.S. GAAS with the International Auditing and Assurance Standards Board's (IAASB's) standards. As part of this project, ASB is also converging U.S. GAAS with the International Standards on Auditing (ISA) issued by the IAASB's statements, to be completed by 2012. The AICPA's redrafted *Consideration of Fraud in a Financial Statement Audit* is one such clarified SAS and is published on the AICPA website at: http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf

[7] Sutherland (1940) described a broad set of acts that constitute white-collar crime, including misrepresentations; manipulations in the stock exchange; commercial bribery; bribery of public officials; embezzlement and misapplication of funds; short weights and measures; and misgrading of commodities, tax frauds, and misapplication of funds in receiverships and bankruptcies.

FIGURE 4
Initial Meta-Model of White-Collar Crime



The Fraud Scale

The fraud scale was developed through an analysis of 212 frauds in the early 1980s (Albrecht et al. 1984). The study was based on data obtained from internal auditors of companies that were victims of fraud. Albrecht and his colleagues believed that fraud was difficult to predict and that occupational fraud perpetrators, as a group, were difficult to profile. Based on the results of their study, Albrecht et al. (1984) proposed the fraud scale, which relies on two components of the Fraud Triangle, pressure and opportunity, but replaces rationalization with personal integrity. Figure 5 is a visual representation of the fraud scale.

Operationalizing the fraud scale, the degree of fraud risk is determined by jointly considering three criteria—pressure, opportunity, and integrity. For example, in the illustration everything is in

FIGURE 5
Fraud Scale

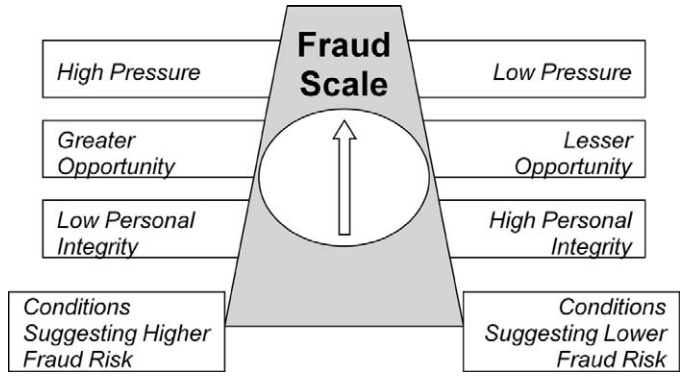
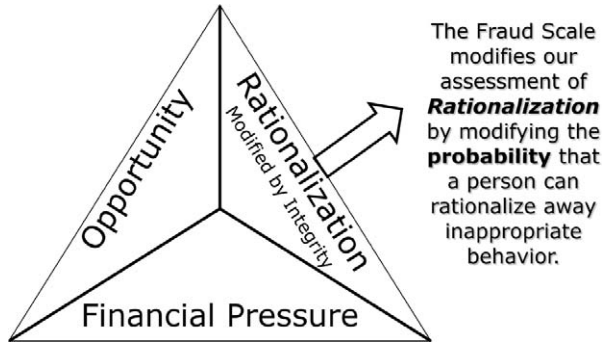


FIGURE 6
The Impact of the Fraud Scale on the Fraud Triangle



"balance" and the fraud risk is neutral, but when situational pressures and perceived opportunities are high and personal integrity is low, fraud is more likely to occur than when the opposite is true.

The benefit of examining integrity is that an individual's integrity can be inferred from past behavior. For example, a person's integrity is reflected in his decisions as well as in his decision-making processes. More importantly, personal integrity affects the probability that an individual may rationalize inappropriate behavior. For example, persons with greater integrity would be less likely to form rationalizations for justifying inappropriate behavior. From that perspective, integrity is a refinement of the rationalization construct as presented in Figure 6.

The Acronym M.I.C.E.

Not every fraud incident seemingly involves a non-shareable financial need. Consider the following two examples. First is the case of Thomas M. Coughlin, former vice-chairman of Walmart and personal friend of founder Sam Walton. On January 24, 2005, Coughlin resigned from Walmart's Board of Directors among allegations of fraud and deceit. Documents reviewed by the *Wall Street Journal* suggest that Coughlin periodically had subordinates create false invoices to get Walmart to pay for his personal expenses (Bandler and Zimmerman 2005). The questionable activity spanned a period of more than five years and involved dozens of transactions including hunting vacations, a $1,359 pair of alligator boots custom made for Coughlin, and a $2,590 dog pen for Coughlin's Arkansas home. According to the article, Walmart uncovered questionable transactions totaling between $100,000 and $500,000. In the year immediately prior to his resignation, Coughlin's annual compensation totaled more than $6 million. Given his annual compensation, Coughlin's need does not appear consistent with Cressey's non-shareable financial pressure. The theoretical models and evaluative frameworks discussed thus far are unable to explain Coughlin's apparently irrational choice to commit the fraud.

The second case is that of Dennis Kozlowski and Mark Swartz, the former CEO and CFO of Tyco International, respectively. On June 17, 2005, a Manhattan court found the former executives guilty of stealing $170 million from Tyco through loan program abuse and unauthorized bonuses. They also took an additional $430 million by artificially inflating the company stock through misstated financials (White 2005). Aside from the sheer magnitude of the fraud, is the notoriety and excesses of Kozlowski's lifestyle. In addition to the executive compensation, the former CEO routinely had the company pay for rare art, parties, and sports activities unrelated to Tyco business. The Fraud Triangle component of non-shareable financial need is absent in this situation.

Ramamoorti et al. (2009) examine executive white-collar crime and attempt to understand why wealthy, influential, and prominent members of society would risk becoming involved in white-collar crime. They conclude that social status comparisons may suffice for motivation in the commission of fraud. Similarly, Coleman (1987) suggests that a culture of competition may be a motivating factor for many white-collar criminals. Coleman implies that wealth and success become more than goals, but rather a part of the identity of the individual. Therefore, the pressure may derive from a need to preserve an identity image as well as a financial need. A significant opportunity for future research might involve exploring the various pressure sources, in addition to financial pressures, specified in the Fraud Triangle.

Recent discussions have suggested that the motivations of fraud perpetrators may be more appropriately expanded and identified with the acronym M.I.C.E. (Kranacher et al. 2011):

M = money
I = ideology
C = coercion
E = ego (entitlement)

M-I-C-E modifies the pressure side of the Fraud Triangle, as it provides an expanded set of motivations beyond a non-shareable financial pressure. Money and ego appear to be common motivations for fraud. Case histories of Madoff, Stanford, Enron, WorldCom, Adelphia, Phar-Mor, and ZZZZ Best provide examples where the convicted perpetrator appears to be motivated by ego or entitlement, as well as money.

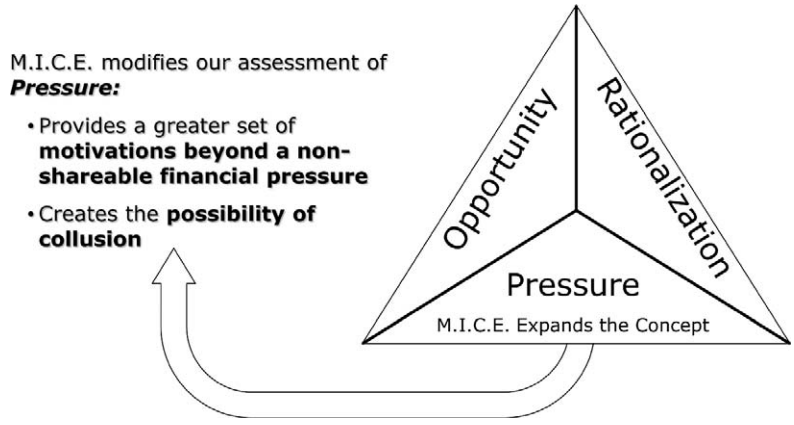
Ideology is probably a less-frequent motivation for white-collar crime, yet examples come to mind. First, tax evasion, where the perpetrator cites that "taxes are unconstitutional" or "I pay enough taxes," might be examples. A second and more frightening example is that of terrorism financing. Excise tax evasion schemes and money-laundering rackets designed, not to make the perpetrators wealthy, but rather to fund a terrorist organization, have been observed. From an ethical perspective, with ideology, the end justifies the means.[8] Perpetrators steal money or participate in a fraud act or financial crime using the argument that they are achieving some perceived greater good.

A recent and specific example of this type of fraud occurred at the First Security Trust & Savings bank in Chicago from September 2004 to February 2009. Jeffrey Gonsiewski altered the terms of at least 100 loans for borrowers struggling to make mortgage payments. The alterations made the loans appear current, and prevented foreclosure and other actions against borrowers. In one specific case, Gonsiewski simply wrote-off $100,000 of interest owed by one borrower. In other cases, he made loans where sufficient collateral did not exist. Gonsiewski, whose actions cost the lending institution $5.5 million, did not benefit personally from the fraud. Nonetheless, Gonsiewski was sentenced to 63 months in prison and ordered to repay $5.2 million (Yerak 2010). Gonsiewski's fraud appears to be motivated by ideology rather than personal benefit.

Coercion describes the condition where an individual is unwilling, but nonetheless pressured into participating in a fraud scheme. As an example, referring again to the Walmart–Coughlin case, Patsy Stephens sued Thomas Coughlin claiming that she was coerced into submitting vouchers and laundering the money through her own bank account (White 2008). Similarly, Betty Vinson, a convicted WorldCom mid-level accountant, reports that she was ordered to make false accounting entries (Pulliam 2003).

[8] Some philosophies such as Immanuel Kant's ethical approach, Deontologism, posit that the end never justifies the means.

FIGURE 7
The Impact of M.I.C.E. on the Fraud Triangle



Like the Fraud Triangle, the M.I.C.E. construct oversimplifies fraudulent motivations. Furthermore, some motivations fit multiple categories. Nevertheless, as a teaching device and a research tool for identifying motivators, modifying the non-sharable financial needs described by Cressey (1950), M.I.C.E. is easily remembered and provides an expanded framework to examine pressure (motivation).[9] Consistent with Ramamoorti et al. (2009), the construct reminds instructors and students that motivations are complex. M.I.C.E. also allows for the possibility of collusion, which, technically, Cressey's non-sharable financial need does not. With regard to financial reporting fraud, the pressure criterion of the Fraud Triangle has been adjusted to focus on motivators such as monetary incentives, bonuses, and/or stock options. While top executives clearly feel pressure to deliver solid financial results, it is not the non-shareable individualized pressure described by Cressey (1950). The impact of M.I.C.E. on the Fraud Triangle is presented in Figure 7.

The Fraud Diamond: Adding the Fraudster's Capabilities

Wolfe and Hermanson (2004) argue that the Fraud Triangle could be enhanced to improve both fraud prevention and detection by considering a fourth element, capability. In addition to addressing incentive, opportunity, and rationalization, the authors' four-sided fraud diamond gives consideration to an individual's capability, which is described as an individual's personal traits and abilities that play a major role in whether fraud may actually occur. The Fraud Diamond modifies the opportunity side of the Fraud Triangle, because without the capability to exploit control weaknesses for the purpose of committing and concealing the fraud act, no fraud can occur.

Wolfe and Hermanson (2004) examine evidence that suggests that many frauds, especially some of the multibillion-dollar ones, would not have occurred without the perpetrator(s) having the right capabilities. As described by the authors, opportunity opens the door to fraud, incentive and rationalization draw the fraudster closer to the door, but the fraudster must have the capability to recognize the opportunity to walk through that door to commit the fraudulent act and conceal it.

[9] Prior research (e.g., Beasley et al. 1999; Beasley et al. 2010) has suggested a greater set of motivations for white-collar crime, but to date the effect on the Fraud Triangle model has only been informally suggested.

The anti-fraud professional seeking to thwart a potential fraud then must evaluate how the current operational environment lends itself to manipulation. The essential traits thought necessary for committing fraud, especially for large sums over long periods of time, include a combination of intelligence, position, ego, and the ability to deal well with stress. The person's position or function within the organization may furnish the ability to create or exploit an opportunity for fraud. Additionally, the potential perpetrator must have sufficient knowledge to understand and exploit internal control weaknesses and to use position, function, or authorized access to his or her advantage. The largest frauds are committed by intelligent, experienced, and creative people with a solid grasp of company controls and vulnerabilities. This knowledge is used to leverage the person's responsibility over or authorized access to systems or assets. This type of person has a strong ego and great confidence that he/she will not be detected, or he/she believes that he/she could easily talk him/herself out of trouble if caught.

Additionally, committing a fraud and managing the fraud over a long period of time can be extremely stressful (Pavlo and Weinberg 2007). Therefore, in addition to being knowledgeable and confident, a successful fraudster also deals well with the stress of committing and concealing the fraud.

In the context of the Fraud Triangle, capability modifies the opportunity construct by limiting opportunity to a small set of individuals thought to have the necessary capability. Thus, capability likely affects the probability that an individual will be able to exploit opportunities in the control environment of the organization (see Figure 8).

Predators versus the Accidental Fraudster

The typical fraudster is often depicted as a first-time offender, middle-aged, well-educated, trusted employee, in a position of responsibility, and/or considered a good citizen through work in the community (ACFE 2009; Ramamoorti et al. 2009). The Fraud Triangle suggests that the perpetrator has a non-shareable problem that is grounded in financial shortcomings, and when aligned with opportunity and rationalization, an otherwise good citizen succumbs to committing fraud. This person might be characterized as the *accidental fraudster*. Notwithstanding the fraud act, the accidental fraudster is considered to be a good, law-abiding person, who under normal circumstances would never consider theft, break felonious laws, or harm others. When discovered, family members, fellow employees, and others in the community are surprised or even shocked by

FIGURE 8
The Impact of the Fraud Diamond on the Fraud Triangle



the perpetrator's alleged behavior. Cressey's Fraud Triangle hypothesis helps the anti-fraud community understand the accidental fraudster.

However, the actions of some fraud and financial crime perpetrators are more closely aligned with the behavior of a *predator*. Consider for a moment this heart-wrenching real-world example (Riley and Frande 2010). A ten-year-old boy is strangled by his father for life insurance money and is left on the side of the road near a lake. To cover up the murder, the father starts a fire in his home and blames his son for accidentally starting the fire. He states that his son ran away after starting the fire and he tearfully pleads on television for his son's safe return. At the time, no one except the father knew that his son was dead. The father set up the crime (premeditation) by talking with others about his son's propensity to play with matches, and he placed matches under the couch seat cushion where his daughter discovered them during routine cleaning. The fire allowed the father to collect additional insurance proceeds related to the home structure and contents. The scheme was perpetrated to repay his most recent former employer as restitution for a fraud that he had committed. The employer had agreed to desist from filing charges or making any public disclosures of the fraud, provided that he reimbursed the company for the missing funds.

What the employer did not know is that this incident was the third time the man had perpetrated a fraud. In the prior incidents, previous employers had quietly terminated the man after discovering the fraud. The choices made by each of his former employers allowed him to quietly move on to his next fraud scheme and eventually create the ultimate victim, his own son. The father was a predator. The predator seeks out organizations where he/she can start to scheme almost immediately upon being hired. At some point, many accidental fraudsters, if not caught early, move from behavior characterized by the accidental fraudster to that of a predator.

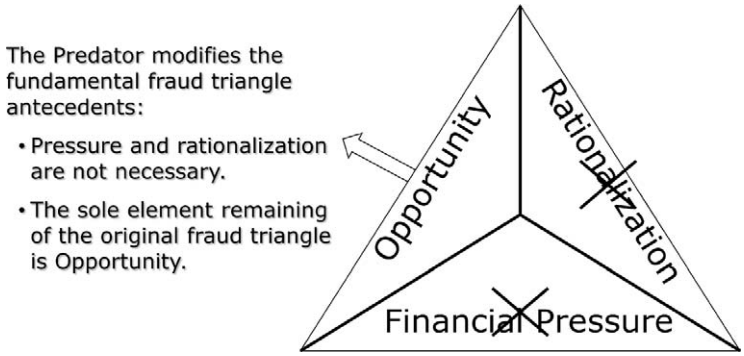
In that regard, Cressey (1950, 1953) observed that a fraudster's internal moral conflict often appears to be a temporary dilemma. After the criminal act has taken place, especially if the fraud has taken place for a long period of time, the rationalization will likely be abandoned or cognitively dismissed. As the act is repeated, the perpetrator becomes de-sensitized. One hallmark of occupational fraud and abuse offenders is that once the line is crossed, the illegal act becomes more or less continuous until it is detected (ACFE 2010; Beasley et al. 1999; Beasley et al. 2010). A white-collar criminal might begin the fraud act with the thought that he/she will stop; however, after the initial effort is successful, the individual will usually continue the act beyond the point where the harm can be reversed. Interestingly, Sam E. Antar, former CFO of Crazy Eddie, takes exception with the concept whereby one moves from being an *accidental fraudster* to a *predator*. Antar refers to accidental fraudsters as crossovers, and to predators as born crooks (Simoleon Sense 2010). No matter the descriptor, the costs borne by the victims and society at-large for predator fraudsters are real (Cardwell 1960).[10]

The concept of the predator also applies to fraudulent financial reporting. Financial statement fraud perpetrators often appear to start as accidental fraudsters by managing earnings, trying to buy time for their organization until conditions improve. But sooner or later, managing earnings gives way to financial reporting fraud, and the accidental fraudster becomes a predator. With regard to the Fraud Triangle and predators, as depicted in Figure 9, pressure and rationalization play little or no role because the predator needs only opportunity.

Instead, arrogance and a criminal mindset replace the original Fraud Triangle's antecedents of pressure and rationalization, and we are left with the elements as they pertain to the predator, as shown in Figure 10.

[10] Rather than using the term "predator," Cardwell (1960) provides a limited description of the "repeater": a professional thief who has "executed some of the largest thefts and ha[s] given professional auditors some of their rudest shocks after thoroughly casing the company, its records, and personnel before developing intricate theft and concealment schemes."

FIGURE 9
The Impact of the Predator on the Fraud Triangle



Predators may be individuals or organizations. Some organizations—drug traffickers, organized criminals, terrorist financers—are deliberately established for a nefarious purpose, and use complex frauds and financial crimes, such as money laundering, to conceal their criminal activity. These activities often involve many individuals, organizations, or shell companies, and span multiple jurisdictional boundaries. Predator-like crimes include conspiracy, RICO violations, money laundering, and mail and wire fraud.

Most fraud literature fails to recognize predators focused on criminal activities. Reference to predators, as opposed to accidental fraudsters, helps educators and researchers to better understand and identify the deliberate acts and motivations of these types of perpetrators. Predators are better organized, have more complex concealment schemes, and are better prepared to deal with auditors and other oversight mechanisms (Kranacher et al. 2011). Finally, because the central focus of the predator is opportunity, risk assessment centered on pressure and rationalization is unlikely to identify predator schemes.

Using opportunity as the common element allows us to see the emergence of a new Fraud Diamond (as illustrated in Figure 11), one that helps to explain the two sides of fraud—the accidental fraudster and the predator.

FIGURE 10
Attributes of the Predator

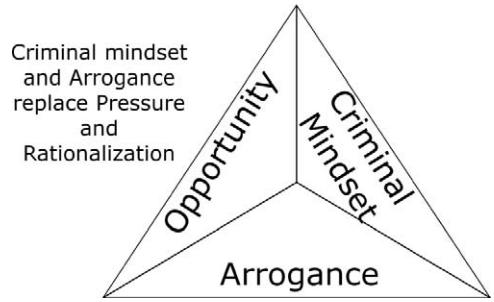
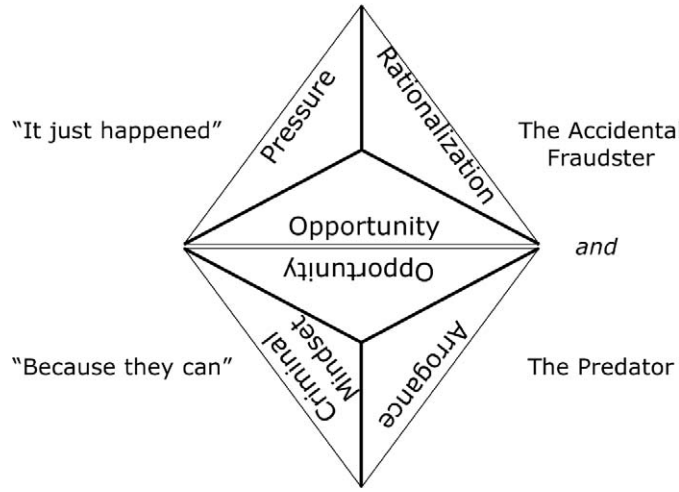


FIGURE 11
The Accidental Fraudster versus the Predator
New Fraud Diamond Emerges With a Common Element



A-B-C ANALYSIS OF WHITE-COLLAR CRIME

While the aforementioned research and theories modify the elements of the Fraud Triangle, the A-B-Cs of Fraud model modifies the probability vector that the expanded antecedent conditions of the Fraud Triangle will result in fraud.

Ramamoorti et al. (2009) propose the A-B-C model for the analysis and categorization of fraud: a bad *A*pple, a bad *B*ushel, and a bad *C*rop. The *bad apple* is an individual, the *bad bushel* addresses collusive fraud (which is also often associated with management override—see Silver et al. 2008), and the *bad crop* refers to cultural and societal mechanisms that influence the relative incidence of fraud. Ramamoorti et al. (2009) note that based on findings from the ACFE (2010), the individual, or *bad apple*, is approximately between the ages of 45 and 55, has a college degree, has been with the company for 10 to 15 years, and generally has a clean past. The *bad bushel* suggests that certain group dynamics encourage or facilitate fraud, and is perhaps exemplified by collusive fraud.

One of the significant contributions of Ramamoorti et al. (2009) is the concept of the *bad crop*, which suggests a deficiency of morals at the top of the organization, and this deficiency is pervasive throughout the organization and possibly culture and society. With regard to bad crops, the Merriam-Webster's dictionary defines an epidemic as:

> Affecting or tending to affect a disproportionately large number of individuals within a population, community, or region at the same time; excessively prevalent; or contagious.

This description seems to describe white-collar crimes that sometimes come in waves, such as stock options backdating. According to Lie (2005, 2010), backdating is the practice of marking a document with a date that precedes the actual date. Employee stock options (ESOs) are usually granted "at-the-money," meaning that the option's exercise price equals the market price of the underlying stock on the grant date. Backdating allows executives to choose a prior date when the market price was lower, thereby artificially inflating the value of the options to the recipient. For

example, assume a CEO is granted options on December 31, 1998, but the options are dated as of October 1998 when the stock price was only $30. Further assume that the number of options granted was 250,000, the exercise price was $30 (same as the market price in October), and the year-end stock price was $85. Given backdating, the intrinsic value of the options at the end of the year is ($85–$30) × 250,000 = $13,750,000. In comparison, had the options been granted at the year-end price of $85 when the decision to grant the options was made, the year-end intrinsic value would be zero.

The timing and grant price of stock option issuances by corporations to executives has been a subject of academic research since the 1990s. Initially, Yermack (1997) and Aboody and Kasznik (2000) assumed that the timing (dating) of stock options was oriented around good news and bad news. Lie (2005) suggested that the timing was set to exploit market-wide price depressions that nobody, including insiders, could predict, leading to a conclusion that at least some of the option grants were retroactive. The backdating scandal publicly ensnared as many as 200 public companies and is estimated to have cost more than $10 billion. Anecdotally, it is also believed that perhaps hundreds more companies privately investigated and resolved the issue of options backdating.[11]

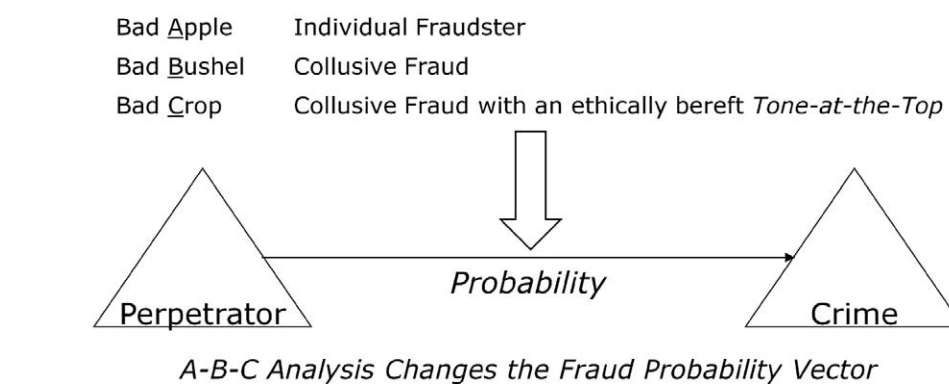
Given the pervasiveness of the options backdating fraud, it has the characteristics of an epidemic. One might wonder how such an illegal practice began. In fact, Hulbert (2007) suggests an answer in the title of the research, "Why Backdated Options Might Be Contagious." According to Bizjak et al. (2007), the probability that a company would start the practice of backdating rose by a third to a half if one of its directors was also on the board of a company that was already backdating.

The epidemic potential of financial fraud is not limited to the issuance of options. Other examples that demonstrate the ability of a fraudulent act, particularly financial fraud, to reach epidemic levels include:

- The 2007–2008 sub-prime mortgage crises will cost Americas hundreds of billions of dollars. Although fraud is not considered a major cause at this point in time, a failure of corporate leadership to properly assess business risks was an inherent issue. The lack of due diligence in loan origination was pervasive, and represented an epidemic in underwriting credit where the loan was not economically justified.
- Prior to the current mortgage crisis, in the early 1980s the American public suffered through, and paid for, the savings and loan (S&L) crisis. During that crisis, it was estimated that 1,700 savings institutions and almost 500 thrifts failed. That crisis, like the sub-prime mortgage crisis, was tied to a severe over-valuation of real estate. However, at least part of the S&L problem was the exploitation of generally accepted accounting principles related to goodwill.
- In 2005, KPMG agreed to take responsibility for its ex-partners' actions related to the firms offering tax shelter services. In the process, the Department of Justice built a case for obstruction of justice and the sale of abusive tax shelters. Attorney General Alberto Gonzales, in a written statement, indicated that KPMG's tax shelters enabled wealthy clients to evade $11 billion in taxes they owed on income and capital gains, and brought the firm at least $115 million in fees. Seventeen former KPMG tax partners were indicted by the Department of Justice for defrauding the IRS by creating four fraudulent tax shelters. KPMG itself was not indicted, but did agree to pay a $456 million penalty, accepted an independent monitor of its operations, and acknowledged wrongdoing to avoid an indictment.

[11] Backdating ESO grants is not necessarily illegal if the following conditions hold: (1) no documents have been forged, (2) backdating is clearly communicated to the company's shareholders, (3) backdating is properly reflected in earnings, and (4) backdating is properly reflected in taxes. Unfortunately, in recent years these conditions were rarely met, making backdating of grants illegal in most cases.

FIGURE 12
The Impact of the A-B-Cs of Fraud on the Fraud Triangle



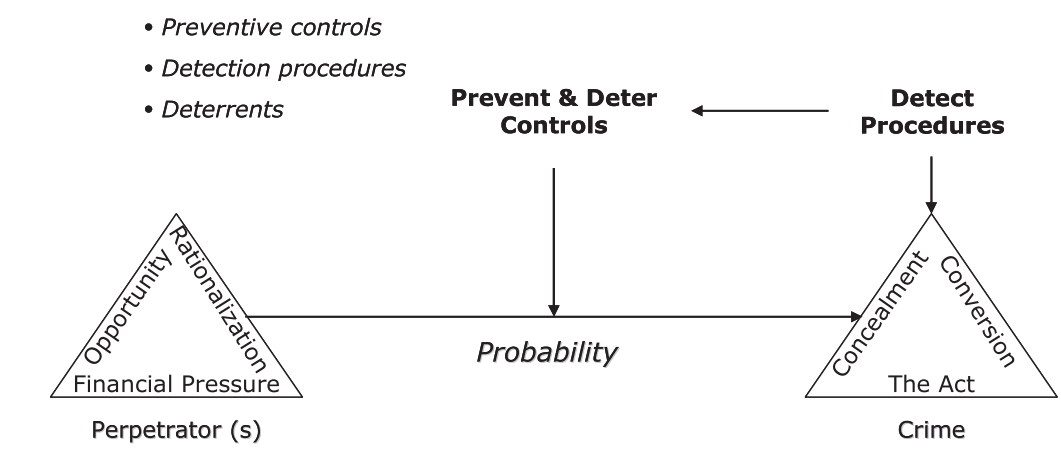
Where do corporate management and governance leaders get ideas that may lead to pervasive fraudulent acts and unsound business practices? Once a practice, even an illegal one, becomes trendy, it may create pressure on companies competing for the same managerial talent, the same stock price appreciations, and the same customers to at least consider doing the same. Fraud epidemics are consistent with the concept of a bad crop, but have not been well researched as a phenomenon. Related to the meta-model described herein, the A-B-Cs of Fraud model modifies the probability that the antecedent conditions of the Fraud Triangle, as expanded herein, will result in fraud acts and financial crime. This impact is depicted in Figure 12.

THE ANTI-FRAUD PROFESSION'S RESPONSE

The meta-model also provides a framework for evaluating the anti-fraud profession's response. Generally, anti-fraud measures can be described as efforts at prevention, deterrence, and detection. Prevention lessens the probability of fraud primarily through the reduction of opportunity. In contrast, deterrence refers to creating environments where fraud is less likely to occur (i.e., less probable). Anecdotally, the two most powerful deterrents are believed to be the fear of getting caught (detection) and the fear of repercussions (punishment). Regarding the anti-fraud environment, examples of deterrence include efforts to create workplace integrity, ethical tone at the top, whistleblower hotlines, and whistleblower protections. Detection procedures are used primarily to discover the crime, but if employees are aware that rigorous detection procedures are in place, they may be, in fact, a form of deterrence (the increased probability of being caught reduces the probability that an individual will act). Another valuable aspect of the meta-model is that it identifies characteristics that can be tested for influence on the probability of the fraud vector. As presented in Figure 13, the overall goal of the anti-fraud profession's response is to lessen the probability of fraud acts and financial crimes—that is, lower the probability of the fraud vector.

The meta-model provides a framework for discussing the intended influence of individual anti-fraud efforts, as well as a model for constructing a cohesive and coordinated anti-fraud environment. Generally, any well-implemented anti-fraud action will affect more than one aspect of the fraud vector; however, each has a primary focus. Each of these anti-fraud measures is discussed in general and in the context of the meta-model. The following discussion provides an instructional structure in which to discuss the anti-fraud professional's response and evaluate the primary focus

FIGURE 13
The Anti-Fraud Profession's Response



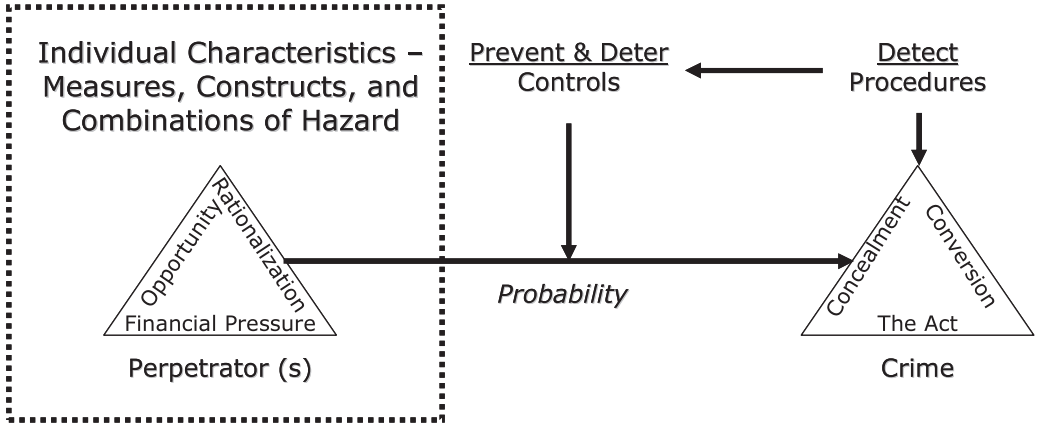
of each response in influencing the fraud vector. Common anti-fraud measures are identified within their primary Fraud Triangle influence (preventive, deterrence, and detection) and briefly discussed in the context of a fully ascribed meta-model (Figure 14).

Prevention

Internal Controls

Accounting instruction traditionally has focused on internal controls—particularly the segregation of duties—as a key anti-fraud mechanism, but internal controls are not all encompassing or entirely effective. The lack of effectiveness is because the cost of controls to

FIGURE 14
Fully Ascribed Meta-Model of White-Collar Crime



prevent every fraud, even material ones, is perceived to exceed the benefits. In response, organizations pick and choose those preventive controls believed to provide the greatest benefits, given budgetary constraints.

Another challenge is that stale controls—those outdated by the changing and increasingly complex business environment—render once-robust controls ineffective. Further, those who routinely work within a static set of controls eventually become aware of the vulnerabilities of the system and how those vulnerabilities can be exploited. Even when controls cannot be circumvented by a single individual, controls may be bypassed through collusion and management override.

Controls must also be designed well and implemented effectively. A properly designed control may not be operationally sound. Controls can be non-operational because of employees who do not follow established policies and procedures, or managers who override the system (COSO 2009).

Internal controls deal primarily with the opportunity aspect of the crime. The proper use of a control environment can influence the potential fraudster's evaluation of the possibility that the act could successfully be committed and concealed. Even if the perpetrator is able to carry out the act, the likelihood of discovery is enhanced through the internal control environment, thereby negatively influencing the concealment requirement of the fraud vector.

Sensitizing to Fraud and Setting an Ethical Culture

As a direct attack on the rationalization element of the Fraud Triangle, anti-fraud professionals have sought to create work environments where ethical sensitivity causes an individual contemplating a fraud to have second thoughts. By routinely encouraging ethical thinking, the potential fraudster has a greater degree of cognitive dissonance to overcome.

Violations of ethics, trust, and responsibility are at the core of fraudulent activities. Ethics addresses rationalization and, to a certain extent, the pressure associated with fraud by considering the conditions under which an action may be deemed right or wrong. By explicitly considering the ethics of a decision, one may be able to persuade a potential fraudster of the error of his/her ways *before* the person initiates his/her first fraudulent act. After an individual commits fraud, that person seldom "self-reforms." Michael Josephson, president of the Josephson Institute of Ethics, suggests several questions that may help to determine whether you are on a slippery slope toward a bad ethical decision.[12]

Generally, the questions proposed by Josephson ask that the decision maker consider whether he/she would make the same choice if his/her family members were present and if the decision was made public. The decision maker should also feel that those he/she admires would be impressed by his/her choice. Finally, the decision maker should feel that the decision is fair even if it were applied to him/her. If the decision maker is able to agree with these conditions, then the decision is not likely in violation of an ethical standard. Providing ethical support should reduce the probability that a potential first-time offender would be able to rationalize his/her actions.

Sutherland (1983) also has influenced current efforts to develop an ethical corporate culture—including "tone at the top"—as a means of deterring fraud and corporate malfeasance. He argues that dishonest employees, especially those in positions of authority within the organization, will eventually infect a portion of honest ones. Conversely, Sutherland's theory suggests that honest employees might also influence those who are dishonest. An environment in which ethics are valued will provide additional deterrence to the potential fraudster because such an environment will make concealment difficult and, once caught, punishment certain.

[12] Adapted from Berkowitz (2002).

Deterrence

Fraud deterrence refers to creating environments in which people are discouraged from committing fraud. The 2005 U.S. Federal Sentencing Guideline Manual defines deterrence as a clear message sent to society that repeated criminal behavior will aggravate the need for increased levels of punishment with each subsequent recurrence. Fraud deterrence is enhanced when (1) the perception of detection is present and (2) potential perpetrators recognize that they will be punished when caught. Anti-fraud deterrence techniques and controls (direct and indirect) include, but are not limited to, the following:

- strong tone at the top
- robust ethical culture
- appropriate control environment
- meaningful code of conduct
- open communications with employees, vendors, suppliers, and customers
- employee activity monitoring
- whistleblower hotlines
- whistleblower protection
- perpetrator punishment protocol
- monitoring of contractual parties
- proactive fraud auditing

The deterrence fabric involves all corporate governance professionals, including the board of directors, audit committee, top management, and external and internal auditors (see NIJ 2007).

The need to emphasize deterrence is supported by prior research findings. Hollinger and Clark (1983) found that a perceived certainty of detection is inversely related to employee theft. That is, as the expectation increases that theft will be detected, the likelihood that an employee will engage in deviant behavior decreases. The primary deterrent is believed to be the fear of getting caught, followed by the fear of punishment.

Deterrence also may be accomplished through a variety of efforts associated with internal controls and ethics programs that create a workplace of integrity and encourage employees to report potential wrongdoing. Such actions increase the perceived likelihood that an act of fraud will be detected and reported.

Fraud deterrence can also be achieved through the use of continuous monitoring/auditing software tools. Again, the overriding theme necessary for an effective deterrent is to put in the mind of the fraudster that detection is likely, thereby reducing the chances of an effective conversion.

Detection

Assessing Fraud in a Financial Statement Audit

A key aspect in detecting fraud is to establish an audit plan designed to help the auditor uncover vulnerabilities in the system that may give rise to material misstatement. The PCAOB's AU Section 316, *Consideration of Fraud in a Financial Statement Audit*, and the AICPA's redrafted SAS, *Consideration of Fraud in a Financial Statement Audit*, provide guidance for conducting an audit with the intent of uncovering fraud. Kranacher et al. (2011) observed that fraud, primarily financial statement fraud, has been a significant concern of the auditing profession, the PCAOB, and the SEC. The scandals of the late 1990s and the early 2000s—Enron, Adelphia, WorldCom, and Tyco—have increased the pressure on auditors to detect fraudulent financial reporting.

The accounting profession responded in 2002 with SAS No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA 2002b),[13] which provided guidance on assessing and responding to the risk of material misstatement arising from fraud. Consistent with this initial

[13] SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*, is the predecessor to the PCAOB's AU Section 316, *Consideration of Fraud in a Financial Statement Audit*, and the AICPA's redrafted SAS, *Consideration of Fraud in a Financial Statement Audit*.

standard, PCAOB and AICPA continue to provide direction on assessing and responding to the risk of fraud that includes: enhanced professional skepticism, pre-audit fraud brainstorming, assessing the risks or existence of fraud, and responding to identified risks.

Our meta-model informs the professional implementing a fraud-sensitive audit plan by identifying the factors that directly affect the probability of the fraud path. While we have not specifically identified how an auditor might identify certain weaknesses, we have provided a framework for evaluating weaknesses in the work environment. That is, the meta-model can be useful in developing a risk assessment approach based on a current understanding of the antecedents to fraud.

Targeted Risk Assessment

Targeted risk assessment gained a significant prominence as an evaluative and planning tool when it was outlined in detail in *Managing the Business Risk of Fraud: A Practical Guide* (IIA et al. 2008). Rezaee and Riley (2010) and Kranacher et al. (2011) note that the targeted risk assessment process can be described in 10 steps, but that it ultimately evaluates risk in terms of two key attributes: the likelihood and the magnitude of the fraud.

Likelihood is evaluated in the context of the company, industry, and operational environment. For example, certain industries are particularly susceptible to specific types of fraud. Second, the magnitude of the fraud is assessed in terms of the potential impact on the firm's financial performance and condition.

An understanding of the business model and corporate environment is necessary to evaluate the types of fraud inherently available to a potential fraudster, and to assess which are most likely to occur. For example, in 2002 Bristol-Myers Squibb admitted to channel stuffing. This illegal practice is an accounting fraud designed to inflate reported revenues,[14] and generally occurs when a company, such as a wholesaler, sells a narrow list of products and has a relatively small number of customers. Within the pharmaceutical manufacturing industry, channel stuffing is a possible fraud scheme of potentially significant magnitude. With knowledge of the company, the industry, and the operating environment, an assessment of fraud risk can focus on those fraud schemes that are most likely to occur and have the potential to be material.

After the first two questions (probability and magnitude) have been answered, additional questions are intended to guide the risk assessment activity to a complete understanding of the process and controls under evaluation (IIA et al. 2008; Rezaee and Riley 2010; Kranacher et al. 2011). These questions generally deal with how a fraud might be perpetrated, how controls might prevent the fraud from taking place, and evaluating the integrity of the controls. This guides the risk assessor toward the weakest points in the control environment with the highest risks.

From Ramamoorti et al.'s (2009) concept of bad apple, bad bushel, and bad crop, educators and researchers can overlay the targeted risk assessment questions of risk likelihood and magnitude. While the likelihood of a bad apple is greater than that of a bad crop, the magnitude of fraud is generally greater with a bad crop.

Collusive Fraud and Management Override

Collusive fraud and management override are two of the more severe threats to anti-fraud efforts. Consequently, the anti-fraud profession targets areas of potential collusion or management override as especially significant.

[14] Channel stuffing involves the delivery of more product by the supplier than the distributor can sell. Inventories on the books of the distributor increase. This reflects the reality that the supplier is warehousing product with the distributor, and that a true sale has not occurred. Suppliers, however, report the delivery of product as a sale, thereby borrowing revenue and earnings from future periods, because overstocked customers will likely reduce orders or return the merchandise in the future.

The Fraud Triangle generally considers an individual, acting alone. But collusion, including management override of controls, is a central element to most complex and costly frauds and financial crimes (ACFE 2010). Parties involved in collusion may be individuals within an organization, individuals across organizations, or multiple organizations, and often span multiple jurisdictions—local, state, federal, and international. The ACFE's (2008) Report to the Nation indicates that when collusion is involved, dollar amounts associated with fraud losses increase dramatically. The losses caused by individual predators can be substantial, but when those individuals work in concert with others, the damage can be devastating and far more pervasive.

The consideration of collusive and management override fraud is a special case of fraud risk assessment. When collusion is involved, internal controls generally are ineffective (AICPA 2005). The primary internal control of segregation of duties helps to ensure that no individual controls every aspect of a transaction and separates the custody, accounting, and approval functions. While internal controls cannot prevent collusive fraud and financial crimes, they may assist in the detection of such activities. In fact, anti-fraud efforts with regard to management override and collusion are centered on deterrence and detection. For example, independent monitoring may reveal that internal controls have been circumvented through collusion. The AICPA (2005) and Rezaee and Riley (2010) note that proactive fraud detection also includes an active search for collusion and management override. The active search includes an examination of journal entries, estimates, and unusual or significant transactions.

Fraud perpetrated via management override can be very difficult to detect. The AICPA (2005) identifies six key recommendations for the audit committee in performing its duties:

1. Maintain skepticism.
2. Strengthen committee understanding of the business.
3. Brainstorm to identify fraud risks.
4. Use a code of conduct to assess financial reporting culture.
5. Ensure the entity cultivates a vigorous whistleblower program.
6. Develop a broad information and feedback network.

In light of the potential for management override and the significant exposure it represents, many recommend that the audit committee take a proactive approach to management override and collusive fraud. Preventing and detecting collusive management fraud requires searching for fraudulent schemes proactively. In some cases, the knowledge and governance structure necessary for more robust detection may simply be unavailable. Beyond the review of management's fraud risk assessment, Silver et al. (2008) suggest that the audit committee (board of directors in the absence of an audit committee) should consider a self-evaluation.

- Do the internal audit group *and* the audit committee have the knowledge, education, and awareness of the various fraudulent management override and collusive schemes that may be perpetrated by management?
- Has the audit committee reviewed a comprehensive fraud risk assessment, including how collusive fraud and management override schemes are mitigated and detected?
- Have the audit committee members participated in continuing education programs that can prepare them for appraising management's fraud risk assessment?
- Did the audit committee assist in the collusive and management override fraud risk assessment process, or did it rely solely on the internal or external audit group?
- Does the audit committee have direct oversight responsibility of internal audit (as required by the NYSE for public companies), or does the internal audit group report to management?

A proactive approach by the audit committee reinforces the tone at the top stance on fraud, sends a positive signal to all management levels, and acts as a deterrent to those contemplating a

collusive fraud scheme. The perception of potential collusive fraud opportunities and the likelihood of being detected from such a proactive approach may reduce the occurrence of one of the most costly frauds within an organization.

A focus on capability requires that organizations and their auditors understand employees' traits and abilities, especially for those in positions of authority and responsibility. Additionally, the work of Wolfe and Hermanson (2004) demonstrates that the capabilities of top executives and key personnel must be explicitly considered as part of the risk assessment process. Audit committee members, corporate accountants, and auditors must target the personality traits and skills of top executives and others responsible for high-risk areas when planning audits, developing deterrence measures, or designing detection procedures.

Of all exposures to fraud, collusion and management override may be the most extreme. Collusive opportunities where controls are circumvented, or where controls may be set aside by management override, must be directly assessed as an opportunity for fraud. An important distinction here is that collusion works around controls to achieve the opportunity for fraud, while management override voids a control in a specific circumstance. In the latter case, management essentially self-reports that no fraud took place and, as a result, conceals their fraud. Accordingly, any risk assessment—whether for audit risk or fraud risk—must target these aspects of the control environment.

CONCLUSION

Various facets of white-collar crime and its underpinnings are found in accounting curricula as content for course modules, stand-alone classes, and separate programs throughout the country (e.g., NIJ 2007; Curtis 2008; Fleming et al. 2008; Kranacher et al. 2008; Kresse 2008; Sanchez et al. 2007), but no explicit link has been made between the various theories of why individuals commit fraud. In this light, we present a meta-model for fraud theory that helps to provide a framework for instruction to improve understandability in the classroom.

Theoretical models surrounding behavioral aspects of the fraud perpetrator originated in the 1940s and 1950s, and are grounded in the early works of Edwin Sutherland and Donald Cressey. It is important also to understand that early work such as the Fraud Triangle has been expanded and enhanced, as outlined in this article. The continual exploration and discussion of fraud, its causes, and controls are important to the development of accounting, audit, risk management, and anti-fraud professionals, and are worthy of consideration when balancing educational curricula and course content.

Ramamoorti (2008) makes a strong case for the integration of additional behavioral sciences content, including psychology, sociology, criminology, and anthropology, into accounting and anti-fraud curricula. Incidents such as trust violation, motivation, deception, and rationalization are part of human behavior that must be incorporated into the study of fraud. A similar argument can be made for further examination of technology in anti-fraud efforts.

The meta-model is also presented as a framework for identifying potential areas for future fraud research, highlighting open questions with regard to fraudsters' characteristics, understanding combinations of characteristics as antecedents to fraud, and recognizing the effects of these characteristics on the probability of fraud. Using the framework as a foundation, future research could delve into unexplored areas, such as interactions among constructs, mediation and moderation effects of controls, and better tools or approaches to enhance detection procedures. This paper is not meant to be all encompassing as it relates to white-collar crime, sociology, or forensic accounting, but rather it is offered as a foundational resource, recognizing developments within the field that have expanded upon the concept of the Fraud Triangle.

REFERENCES

Aboody, D., and R. Kasznik. 2000. CEO stock option awards and the timing of corporate voluntary disclosures. *Journal of Accounting and Economics* (February).

American Institute of Certified Public Accountants (AICPA). 2002a. *Responsibilities and Functions of the Independent Auditor*. AU Section 316. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2002b. *Consideration of Fraud in a Financial Statement Audit*. Statement on Auditing Standards No. 99. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2005. *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention*. New York, NY: AICPA.

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

Albrecht, W. S., C. C. Albrecht, and C. O. Albrecht. 2006. *Fraud Examination*. New York, NY: Thomson South-Western.

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

Association of Certified Fraud Examiners (ACFE). 2009. *Fraud Examiners Manual*. Austin, TX: ACFE.

Association of Certified Fraud Examiners (ACFE). 2010. *Report to the Nations on Occupational Fraud and Abuse*. Austin, TX: ACFE.

Bandler, J., and A. Zimmerman. 2005. A Walmart legend's trail of deceit. *The Wall Street Journal* (April 5).

Beasley, M. S., J. V. Carcello, and D. R. Hermanson. 1999. *Fraudulent Financial Reporting 1987–1997: An Analysis of U.S. Public Companies*. Durham, NC: COSO.

Beasley, M. S., J. V. Carcello, D. R. Hermanson, and T. Neal. 2010. *Fraudulent Financial Reporting 1998–2007: An Analysis of U.S. Public Companies*. Durham, NC: COSO.

Bell, T. B., and J. V. Carcello. 2000. A decision aid for assessing the likelihood of fraudulent financial reporting. *Auditing: A Journal of Practice & Theory* 19 (1): 169–184.

Berkowitz, A. L. 2002. *Enron: A Professional's Guide to the Events, Ethical Issues, and Proposed Reforms*. Chicago, IL: CCH, Inc.

Berle, A. A., and G. C. Means. 1932. *The Modern Corporation and Private Property*. New York, NY: Harcourt, Brace & World.

Bizjak, J. M., M. L. Lemmon, and R. J. Whitby. 2007. *Option Backdating and Board Interlocks*. Working paper, Portland State University.

Braithwaite, J. 1985. White collar crime. *Annual Review of Sociology* 11: 1–25.

Cardwell, H. 1960. *Principle of Audit Surveillance*. Philadelphia, PA: R. T. Edwards, Inc.

Coleman, J. W. 1987. Toward an integrated theory of white-collar crime. *American Journal of Sociology* 93 (2): 406–439.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2009. *Internal Control—Integrated Framework: Guidance on Monitoring Internal Control Systems*. New York, NY: COSO.

Cressey, D. R. 1950. The criminal violation of financial trust. *American Sociological Review* 15 (6): 738–743.

Cressey, D. R. 1953. *Other People's Money: The Social Psychology of Embezzlement*. New York, NY: The Free Press.

Curtis, G. E. 2008. Legal and regulatory environments and ethics: Essential components of a fraud and forensic accounting curriculum. *Issues in Accounting Education* 23 (4): 535–543.

Festinger, L. 1957. *A Theory of Cognitive Dissonance*. Stanford, CA: Stanford University Press.

Fleming, A. S., T. A. Pearson, and R. A. Riley Jr. 2008. West Virginia University: Forensic accounting and fraud investigation. *Issues in Accounting Education* 23 (4): 573–580.

Hogan, C., Z. Rezaee, R. Riley, and U. Velury. 2008. Financial statement fraud: Insights from the academic literature. *Auditing: A Journal of Practice & Theory* 27 (2).

Hollinger, R. C., and J. P. Clark. 1983. *Theft by Employees*. Lexington, MA: D.C. Heath.

Hulbert, M. 2007. Why backdated options might be contagious. *The New York Times* (January 21).

Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), and Association of Certified Fraud Examiners (ACFE). 2008. Managing the business risk of fraud: A

practical guide. Available at: http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf

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

Keay, J. 1992. *The Honorable East India Company: A History of the English East India Company*. London, UK: HarperCollins.

Kranacher, M. J., B. W. Morris, T. A. Pearson, and R. A. Riley Jr. 2008. A model curriculum for education in fraud and forensic accounting. *Issues in Accounting Education* 23 (4): 505–519.

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

Kresse, W. J. 2008. The Saint Xavier University graduate program in financial fraud examination and management. *Issues in Accounting Education* 23 (4): 601–608.

LaSalle, R. E. 2007. Effects of the Fraud Triangle on students' risk assessment. *Journal of Accounting Education* 25: 74–87.

Lie, E. 2005. On the timing of CEO stock option awards. *Management Science* 51 (5): 802–812.

Lie, E. 2010. Backdating of executive stock option (ESO) grants. Available at: http://www.biz.uiowa.edu/faculty/elie/backdating.htm

National Institute of Justice (NIJ). 2007. Education and training in fraud and forensic accounting: A guide for educational institutions, stakeholders organizations, faculty, and students. Available at: http://www.ncjrs.gov/pdffiles1/nij/grants/217589.pdf

Pavlo, W., Jr., and N. Weinberg. 2007. *Stolen Without a Gun: Confessions from Inside History's Biggest Accounting Fraud—The Collapse of MCI WorldCom*. Tampa, FL: Etika Books.

Public Company Accounting Oversight Board (PCAOB). 2010. *The Auditor's Responses to the Risks of Material Misstatement*. Auditing Standard No. 13. New York, NY: PCAOB.

Pulliam, S. 2003. Ordered to commit fraud, a staffer balked, then caved. *Wall Street Journal Online* (June 23).

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

Ramamoorti, S., D. Morrison, and J. W. Koletar. 2009. *Bringing Freud to Fraud: Understanding the State-of-Mind of the C-Level Suite/White Collar Offender Through "A-B-C" Analysis*. Working paper, Institute for Fraud Prevention.

Rezaee, Z., and R. A. Riley Jr. 2010. *Financial Statement Fraud: Prevention and Detection*. 2nd edition. New York, NY: Wiley.

Riley, R. A., and F. Frande. 2010. Expert guest instructors: Incorporating practicing professionals in the classroom, fraud edge. *Fraud Magazine* (July/August).

Robins, N. 2007. This imperious company: The English East India Company and its legacy for corporate accountability. *Journal of Corporate Citizenship* (Spring).

Sanchez, M. H., K. F. Brown, and C. P. Agoglia. 2007. Consideration of control environment and fraud risk: A set of instructional exercises. *Journal of Accounting Education* 25: 207–221.

Simoleon Sense. 2010. GuestPost: Fraud girl interviews famous financial felon Sam Antar. Available at: http://www.simoleonsense.com/guestpost-fraud-girl-interviews-convicted-financial-felon-sam-antar/

Silver, S., A. S. Fleming, and R. Riley. 2008. Collusive fraud: The audit committee's oversight role. *The CPA Journal* (October).

Smith, A. 1776. *An Inquiry into the Nature and Causes of the Wealth of Nations*. Chicago, IL: The University of Chicago Press (1976).

Snider, L. 1982. Traditional and corporate theft: A comparison of sanctions. In *White-Collar and Economic Crime*, edited by Wickman, P., and T. Dailey, 235–258. Toronto, ON: Lexington Books.

Sutherland, E. H. 1940. White-collar criminality. *American Sociological Review* 5 (1): 1–12.

Sutherland, E. H. 1944. Is white-collar crime crime? *American Sociological Review* 10 (2): 132–139.

Sutherland, E. H. 1983. *White Collar Crime: The Uncut Version*. New Haven, CT: Yale University Press.

White, B. 2005. Ex-Tyco executives convicted. *The Washington Post* (June 18).

White, B. 2008. Former Walmart manager sues Tom Coughlin—for her own misdeeds. *BloggingStocks* (April 1).

Wolfe, D. T., and D. Hermanson. 2004. The Fraud Diamond: Considering the four elements of fraud. *The CPA Journal* (December).

Woodward J. D., Jr., N. M. Orlans, and P. T. Higgins. 2003. *Biometrics: Identity Assurance in the Information Age*. Santa Monica, CA: McGraw-Hill.

Yermack, D. 1997. Good timing: CEO stock option awards and company news announcements. *Journal of Finance* (June).

Yerak, B. 2010. "Robin Hood" banker gets 63 months for fraud. Available at: http://chicagobreakingbusiness.com/2010/12/first-security-trust-worker-sentenced-to-63-months-for-fraud.html

APPENDIX A

Evolution of Fraud Theory PowerPoint Deck: http://dx.doi.org/10.2308/iace-50131.s1.

American Accounting Association