Original Research

WALDEN UNIVERSITY

Strategies to Prevent and Detect Occupational Fraud in Small Retail Businesses

Marquita V. Davis, DBA
Walden University, Minneapolis, Minnesota, United States
ⓘD https://orcid.org/0000-0001-9124-4948

David Harris III, DBA
Walden University, Minneapolis, Minnesota, United States
ⓘD https://orcid.org/0000-0002-0230-8223

Contact: david.harris4@mail.waldenu.edu

Abstract

The objective of this multiple case study was to explore internal control strategies owners of small retail businesses in southeastern Pennsylvania used to prevent and detect occupational fraud. The results of this study indicated that there are areas for action that owners of small retail businesses could take to prevent and detect occupational fraud. Strategies business owners could implement to protect their businesses from occupational fraud include monitoring, tracking employee activity using employee identity documents, separating duties, and communicating with employees. Small business owners serve their communities by focusing on wealth distribution, including donations to local charities that foster economic stability with positive effects on society.

Introduction

Occupational fraud, a term used interchangeably with *employee fraud*, occurs in small businesses where preventative measures to prevent fraud do not exist (Lofland & McNeal, 2014). Unethical employee behavior is a significant factor contributing to occupational fraud (Pierce & Snyder, 2015). Some employees in the retail industry commit occupational fraud by intentionally ignoring shoplifters as they may benefit from the crime by looking the other way; the perpetrator may be compensating the employee for not reporting him or her (Pierce & Snyder, 2015). Fraud against small businesses has serious financial implications, as many small business owners are unable to recover from fraud loss, whether it is theft of inventory or cash (Button et al., 2014).

Retail trade businesses engaged in nonfederal business are small if annual receipts are $7.5 million with less than 200 employees (Small Business Development Center [SBDC], 2017). Small businesses account for 98.2% of the state of Pennsylvania's employers; however, there has been a decrease in the birth of small retail businesses with less than 200 employees within the last 3 years, down to 37.7% (SBDC, 2017). Small businesses are integral to local communities as owners realize the opportunity to create resources, add value, and improve economic conditions (Feldman, 2014). When small business owners become victims of occupational fraud and are not able to recover, the business as well as the community may suffer. We intend to explore to explore strategies small business owners implemented to prevent occupational employee fraud and remain successful.

Trustworthiness in small businesses is often taken for granted because small business owners assume that employees can be trusted and take that trust at face value (Smith, 2016). This naive trust primes the business owners for becoming victims of occupational fraud, leading to asset misappropriation, which continues to be an ongoing problem. What many small business owners may not take into consideration is that women and men commit employee fraud in every industry, equally, with the exception of the banking industry where women outnumber men (Bonny et al., 2015). Thus, an employee motivated to commit fraud may be of any age or gender and convey the perception that he or she is the most trusted employee in the company.

The overall purpose of this study is for small business owners realize that they are not immune to occupational fraud and their internal control procedures should be as effective as their larger counterparts' internal controls. Fraud remains one of the most problematic issues for businesses worldwide (Gullkvist & Jokipii, 2013). Van Gelder and DeVries (2016) argued that despite the ubiquitous nature of employee theft, occupational fraud by ordinary employees is a field that does not generate much enthusiasm by crime researchers. According to Van Gelder and DeVries (2016), most attention is given to high-profile white-collar crimes involving corporate executives despite the fact that occupational fraud occurs more frequently. Occupational fraud has not received the attention required from researchers. The results of this study should prompt small business owners to be more strategic when formulating internal control processes to prevent and deter employee fraud.

Literature Review

Occupational fraud is the deliberate misuse of an employer's assets by an employee (Goldstein, 2015). Disgruntled employees commit occupational fraud or may do so because the opportunity exists. Occupational fraud includes asset misappropriation, cash theft, and financial statement fraud (Goldstein, 2015). The focus of this study will be asset misappropriation in small businesses. Small businesses in Pennsylvania employed 2.4 million employees in 2014 and accounted for 47.3% of the private sector labor force (SBDC, 2017). In Philadelphia County where the research will be conducted, small businesses account for a total of 99% of all businesses with 500 or less employees (SBDC, 2017).

Despite the large number of small businesses in the Southeastern region of Pennslvania, occupational fraud prevention methods are lacking, which could cause small businesses to fail because owners are unable to recover from fraud attacks (Kramer, 2015). The purpose of this study was to explore the strategies that successful small businesses have employed to prevent occupational fraud within their businesses. Asset misappropriation significantly damages small businesses. Hunt and Austin (2014) said that asset misappropriation was the most common type of fraud.

Fraud

Fraud, as suggested by Anand et al. (2015), is a controversial word as it can have several definitions, depending upon what an organization considers ethical or unethical. Anand et al. argued that there are several types of fraud; for example, there is internal employee fraud, also known as occupational fraud, and fraudulent financial statements. In this study, the focus is on internal occupational employee fraud. A fraudster's attitude towards his or her employer could contribute to decisions to commit occupational fraud, which can fluctuate depending on the fraudster's circumstance outside of work (Andon et al., 2015).

Fraud has become one of the most challenging obstacles in economic development to date (Azim & Azam, 2016). Fraud, as opposed to a mere mistake with lower risk, is an intentional act meant to harm an individual's employer (Hamilton, 2016). In overcoming the hesitation of investigating the most insignificant instances of occupational fraud, managers and owners should consider their own thoughts, emotions, and loyalty towards their employees, and more important, their business (Hamilton, 2016). There are significant issues to consider when looking at fraud through the eyes of a small business owner or manager such as personal relationships, or the fact that the fraudulent act may be so minuscule that the fraud is not recognized or reported. Unfortunately, some employees in small businesses are likely to take advantage of their employer's trust and exploit their positions, especially where there is a lack of separation of duties (Ding & Wu, 2014). Petraşcu and Tieanu (2014) reinforced the importance of social change by emphasizing the adverse effects on the entire economy of accounting fraud, which is also the message we intend on sending throughout this study. When small businesses fail, the economy suffers as well as the business. Furthermore, accounting fraud results in substantial financial losses. Financial losses have a snowball effect; they weaken social stability as well as trust in the economy as well as social institutions. Fraud is a direct result of weak internal controls or nonexistent internal controls in some circumstances (Petraşcu & Tieanu, 2014).

Occupational fraud

Occupational fraud, also referred to as employee fraud, is one of the most common crimes committed against small businesses (Kennedy, 2016). Peltier-Rivest and Lanoue (2015) said that asset misappropriation was one of the most frequently occurring occupational fraud schemes among all fraudulent acts. However, occupational fraud not only affects the organization internally, but externally as well (Peltier-Rivest & Lanoue, 2015). The organization will not only lose its assets but also revenue, as well as its reputation. Small business owners are reluctant or slow to place proper protocols for preventing and detecting occupational fraud, leaving them vulnerable to asset misappropriation and other losses. Small business owners may leave such protocols out of employee trainings and onboarding as well, not realizing how critical this element is to their businesses (Henry, 2016).

Asset misappropriation

Fraud, particularly asset misappropriation, has been an ongoing growing concern for business owners when there were no internal controls (Lenz & Graycar, 2016). Asset misappropriation, one of the most common types of occupational fraud is only second to financial statement fraud (Krambia-Kapardis & Papastergiou, 2016). Small businesses often lack internal controls to prevent occupational fraud; as such, they suffer disproportionately large losses (Klein, 2015). Klein said that 85% of occupational fraud instances are due to asset misappropriation. Many small businesses lack adequate internal controls because of the financial responsibility required to implement and maintain the controls (Alleyne & Amaria, 2013). However, by preventing asset misappropriation when losses are so costly to small businesses, the benefits of implementing internal controls outweigh the costs. Additionally, white collar crimes have taken the form of asset misappropriation on the grounds of employee entitlement, notwithstanding the owners' oversight of growing businesses over time (Lenz & Graycar, 2016).

Fraud Triangle

Sociologists and psychologists who determine why criminals commit financial crimes use the fraud triangle. Decision makers in organizations use the fraud triangle to understand, prevent, and detect not only asset misappropriation or fraudulent financial statements, but fraudulent acts committed by all fraudsters (Daigle et al., 2014). When assessing fraud risk exposure, determining who may be potential perpetrators, and developing strategies to prevent asset misappropriation, some decision makers will refer to the fraud triangle to construct the most effective fraud prevention controls (Mihret, 2014). Despite the controversy about to the effectiveness of the fraud triangle model and its use for risk assessment, the auditing profession has formally adopted the fraud triangle as part of Statement on Auditing Standards 99 (Suliman et al., 2014). Bakri et al. (2017) suggested that the fraudulent activity that led to the demise of such companies as Enron, Satyam, and Parmalat were due to the components of the fraud triangle: lack of internal controls, pressure, or incentives to commit fraud as well as rationalizations to commit fraud. Bakri et al. also presented the fraud triangle model in their study as a fraud assessment tool instead of a fraud detection tool, which is how small business owners should be capitalizing on the use of the model, which is to prevent fraud. Taking preventative measures against fraud is less expensive and more efficient than detecting fraud after the act has occurred (Sorunke, 2016).

The fraud triangle is critical in preventing and detecting occupational fraud, perceived pressures, perceived rationalizations, and motivations; however, these perceptions are not all inclusive. Kummer et al. (2015) argued that pressure to commit fraud was an unshareable need, which could be a financial pressure the fraudster does not want to divulge to his or her employer. . An unshareable need, as defined by Dellaportas (2013), occurs when an individual encounters a personal crisis. Conversely, rationalization involved personal ethics, opportunity, and lack of adequate controls within an organization and having the knowledge to commit fraud on behalf of the perpetrator. Dellaportas (2013) suggested that perpetrators tend not to react after committing occupational fraud; instead, they display no reaction or remorse, and later attempt to rationalize their crimes. LaSalle (2007) and Kummer et al. (2015) both argued that opportunity for a perpetrator to commit fraud presents itself when there is a lack of internal controls within an organization. When internal controls are inadequate or nonexistent, this creates a poor workplace environment, which allows the opportunity for occupational fraud to arise (Mui & Mailley, 2015). Bhasin (2013) suggested that without the opportunity to commit occupational fraud, fraud could not exist.

Eaton and Korach (2016) suggested that from a public lens, white collar crime or occupational fraud is the principal reason for lack of trust and approval of businesses as well as the reason for the erosion of businesses over the last three decades. Because occupational fraud is a crime, Eaton and Korach recommended incorporating the fraud triangle in a more extensive criminal profiling operation. The more extensive criminological profile includes personality traits, behavioral analysis, and individual characteristics beyond the fraud triangle model's capabilities. Eaton and Korach posited that knowledge of perpetrators' past personality traits alongside current traits that are within the realm of the fraud triangle's capabilities are far more useful for fighting and preventing employee fraud. A layperson who has no prior behavioral analysis training may have certain personality traits that will go undetected regardless of their knowledge of the fraud triangle. For example, an owner interviewing a potential employee may not realize the demeanor of someone who was previously in an authoritative position with power who was not accustomed to answering to anyone else, instead of doing what they want (Eaton & Korach, 2016). Other traits include cultural hedonism, narcissistic personality disorder, and narcissistic personality tendencies that are features of narcissistic personality disorder (Eaton & Korach, 2016). With these individuals, everything is about them and their needs and wants, without regard to anyone else and as far as they are concerned, rules do not apply to them.

In many instances, researchers refer to the fraud triangle in research studies involving massive financial fraud or occupational fraud cases. For example, Finnerty et al. (2016) referred to the fraud triangle model in their study on large firms with trading futures on the stock market before the fraudulent misconduct. The Sarbanes-Oxley Act of 2002 was a regulatory reform enacted as a response to a decline in accounting ethics and professionalism that revealed financial statement frauds, asset misappropriations, and embezzlements (Lail et al., 2017). Each of the fraud triangle components was key contributors to the financial reporting fraud occurrences that led to multiple system failures (Lail et al., 2017). Finnerty et al. (2016) purported that perpetrators of financial crimes often did not commit financial crimes for 5 years before committing their first financial crime. After multiple consecutive years of successful financial performance, management felt pressured to continue reflecting positive financial performance; thus, they began committing fraud (Finnerty et al., 2016). Financial pressures were one of the key elements Cressey identified in his 1953 fraud triangle model (Finnerty et al., 2016). Finnerty et al. purported that perpetrators of financial crimes often did not commit financial crimes for 5 years before committing their first financial crime. Finnerty et al. also suggested that the perpetrators sit in wait until the perfect opportunity, until they believe no one is watching, and until they believe, their actions will have no consequences.

Leistedt and Linkowski (2016) posited that the fraud triangle identifies two levels for committing fraud, the personal (microlevel) skills, and the networking (macrolevel) skills. The fraud triangle according to Leistedt and Linkowski falls under the microlevel as the elements of the fraud triangle pertain to an individual's actions in his or her environment. Fabrication of results of materials, falsification of records, and plagiarism are crimes that a business owner could assess using the fraud triangle model (Leistedt & Linkowski, 2016). Fraudsters seek opportunities where they know internal controls are ineffective and where there are no ethical boundaries explicitly and efficiently placed (Leistedt & Linkowski, 2016). Leistedt and Linkowski also suggested that ethical policy is a reflection of the tone at the top; management must implement and demonstrate an example of ethical standards. In an environment where unethical behavior is intolerable, where it is punishable, potential fraudsters are less likely to commit fraudulent acts (Leistedt & Linkowski, 2016). Reducing fraudulent occurrences includes reducing or eliminating the opportunity to commit fraud (Azizul-Islam, 2014; Leistedt & Linkowski, 2016). Employees of organizations are not the only perpetrators of fraud; managers are culprits as well, which is a signal of weak internal controls and lack of ethical policy. Management commits fraud for the same reasons as lower level employees, pressure (forced to make the numbers), rationalization ("I had to in order to keep my position"), and opportunity (overriding internal controls; Lightle et al., 2015). Management is responsible for presenting financial statements that are free from error and relied on when assessing an organization's ability to generate cash as well as demonstrating the ability to adapt to economic change (Tsegba & Upaa, 2015).

Pressures, motivations, or incentives to commit fraud
Pressure or motivation to commit fraud often triggers the fraud triangle as purported by Sídoróv (2015). Holtfreter (2015) argued that men and women provide the same rationalization for stealing from their employers. Men and women have maintained that they were borrowing and intended to repay their employers at some time in the future; however, Holtfreter found that the motivations were not the same for men and women. Cressey (1953) found that motivation for men to commit financial crimes was often a result of an unshareable financial need such as a gambling debt or addiction (Holtfreter, 2015). Holtfreter suggested that motivation for women to commit financial crimes was medical expenses or medical expenses for a sick child or family member. Attractive incentives for perform cause management and employees to act unethically. Incentives such as promotion, titles, salary increases, and bonuses are the driving forces that place pressure on the fraudster to at criminally (Sídoróv, 2015). Incentives and recognition could compel management to lie about work they have done or taken credit for work done by others to enhance their reputation (Graham & Cooper, 2013). Newfound recognition could motivate management to commit fraud, which is assessably using the fraud triangle. Graham and Cooper posited that the credit taken should match the recognition, should be

justifiable, and strategically made. Any credits, recognition, or incentives that appear to exceed the actual achievement would be a red flag that the risk of fraud is present. The red flag would indicate that the tone at the top lack ethical standards and practices. The tone at the top should be one that promotes ethical behavior throughout the organization.

Employees are under tremendous pressure to perform well meet personal and organizational goals, a secure position within their organization that forces them to seek opportunities to commit fraud (Mishra & Singh, 2017). For example, management may be under extreme pressure to meet or exceed the expectations of stakeholders who have expectations increasing their stock value. Understandably, management wants to meet those deadlines, make their numbers, and increase profit, but these motives should not prompt fraudulent behavior. Failure to promote an ethical culture from the top increases the opportunity for managers and employees to commit fraud by increasing fraud risk for the organization (Sídoróv, 2015). Mishra and Singh (2017) posited that the fraud triangle provided an understanding of the behavior of employees as well as offered help in determining solutions to prevent future fraud occurrences. Some academic researchers continue to reject the notion that the fraud triangle is a predictive model as opposed to the detection tool that it was formed to be by Cressey (1953). Stone (2015) argued that rationalization and pressure are elements of the fraud triangle that are not predictable and therefore cannot be helpful in fraud risk assessment and prevention. Conversely, Power (2013) asserted that the fraud triangle model was critical in identifying fraud risk factors–potential threats to develop internal controls to prevent and detect financial acts of fraud, discussed later.

Rationalization to commit fraud
Another key, yet the daunting element of the fraud triangle is an employee's rationalization for committing occupational fraud, is internal; thus, it is not predictable, the auditor cannot observe what the fraudster is thinking (Boyle, Boyle, et al., 2015). However, rationalization is a critical element of the fraud triangle that decision-makers cannot overlook when using the fraud triangle model in strategizing to determine fraud risk control procedures. Some individuals who commit financial crimes have a mindset that their actions are acceptable, and they make rationalizations in an attempt to prove to others that their actions were justified. Ishida et al. (2016) posited that rationalization is an attitude that some fraudsters possess a mindset, character, or set of values that allow them to commit fraudulent acts knowingly and willingly without remorse. Ishida et al. (2016) suggested that greater incentives propel individuals to be able to rationalize their unethical acts.

Organizational goals imposed on employees by employers may motivate unethical behavior as purported by Clor-Proell et al. (2015). Employees are either very eager to please their employer or extremely disgruntled for having the responsibility of such difficult goals placed on them, that they use those goals as rationalizations for committing fraud. Employees will generally meet or exceed goals that are easy to meet; conversely, employees will not meet goals that are extremely difficult to meet (Clor-Proell et al., 2015). Clor-Proell et al. also argued that goal difficulty was a signal of the employer's fairness that influenced the employee's willingness to engage in fraudulent activity. Viewing the coast goal as unfair makes it easier for the employees to rationalize their fraudulent actions against their employer (Clor-Proell et al., 2015). The commission of occupational fraud and the rationalization of fraudulent activity are not limited to lower level employees; management is guilty of identical behavior. Morgan and Burnside (2014) posited that when the tone at the top does not enforce ethical behavior, an opportunity is present for managers to rationalize fraudulent behavior. In an unethical environment, emphasis is on financial performance and stock prices where managers will do what they feel necessary to meet financial obligations (Morgan & Burnside, 2014). Management may also use the excuse that "everyone lies and cheats," convincing themselves that their fraudulent actions are rational and acceptable (Morgan & Burnside, 2014).

Opportunity to commit fraud
Because the opportunity to commit fraud represents a weakness in internal controls, the fraud triangle is most useful when determining the most effective internal controls to prevent and detect occupational fraud (Daigle et al., 2014). Boyle, Boyle, et al. (2015) posited that the opportunity to commit fraud within an organization is ever-present and an organization's internal controls primary function should be to address the opportunity component of the fraud triangle. For this reason, it is key that small business owners address the matter of immediate opportunity for occupational fraud attacks within their businesses. More important, it is essential that small business owners realize the risk in not using the fraud triangle model during fraud risk assessments. In the decomposition of fraud risk assessment using the fraud triangle, researchers assess each component separately (Fortvingler & Szívós, 2016). Each element standing alone, on its own account could increase the likelihood of fraud when the decision makers utilize the fraud triangle as an assessment tool. Favere-Marchesi (2013) suggested that risk assessments split components of attitude (rationalization), opportunity, and incentives (pressures) into separate categories. Favere-Marchesi posited that assessing fraud risk by considering each element independently produced more accurate fraud risk prevention and detection protocols. Application of the fraud triangle has become vital in fraud risk assessment, so much so, that according to Lin et al. (2015) fraud risk factors are based on the elements of the fraud triangle. Because the fraud triangle components explain why fraud is committed, Lin et al. (2015) suggested that understanding of the fraud triangle is essential for purposes of evaluation and prevention of fraud.

Weak internal controls or the lack of internal controls causes organizations to be vulnerable to asset misappropriation and other types of fraudulent attacks. Because opportunity, pressure, and rationalization are all present when fraudulent activity occurs, it is necessary for external auditors to utilize the fraud triangle model in conjunction with other fraud risk assessment measures. When management in organizations faces pressures to perform financially, there is an incentive to commit fraud, and external auditors must be aware of these risks (Schnader et al., 2015). Because fraud occurs at various levels and has many features, it is imperative to focus on the underlying cause, the fraud triangle, to mitigate fraud (Liu et al., 2015). Liu et al. (2015) also argued that mechanisms to prevent unethical behavior, increase internal control strengths, and communication are within understanding of the fraud triangle. Stone (2015) assertions are in direct conflict with authors such as Lin et al. (2015), Favere-Marchesi (2013), and Mishra and Singh (2017) who all posited that the fraud triangle is an effective tool for fraud prevention. Despite the dominance in fraud literature existing about to the fraud triangle, authors Boyle, DeZoort, et al. (2015) suggested that the original fraud triangle model undergo modification to be of more value to those in fraud risk management. Boyle, DeZoort, et al. (2015) also suggested combining the triangle with other models such as the fraud diamond that includes a capability component (Manning et al., 2016). Azizul-Islam (2014), Leistedt and Linkowski (2016), and Bhasin (2013) suggested that opportunity was the most significant element of the fraud triangle and removal of opportunity to commit occupational fraud would prevent fraud occurrence.

Preventing and Detecting Occupational Fraud

Small organizations are proportionately unprepared for and vulnerable to experiencing occupational fraud (Gilmore-Allen, 2015). Because occupational fraud is so predominant, it is essential that small business owners ensure there are practices in place that prevent and detect the fraudulent issues quickly (Peters & Maniam, 2016). Two effective methods to prevent and detect occupational fraud are to implement internal controls such as ethics and fraud training that could prevent fraud (Peltier-Rivest & Lanoue, 2015) and implement mandatory detection methods such as whistleblowing (Dhamija, 2014).

Preventing occupational fraud
Preventing fraud is economically beneficial to society in addition to creating an ethical corporate structure (Mishra & Singh, 2017). Vrij et al. (2014) conducted a study on interviewing witnesses, soliciting reliable

information, and their propensity to offer accurate information after a crime has been committed. This probing in voluntary interview form is a technique that small business owners could employ during the hiring process. Owners can ask potential employees who are probing interview questions, not only to gain insight of the interviewee's fitness for the open position but their psychological state of mind as well. The interviewers may begin with open-ended questions to build rapport and move on to closed-ended question to ask more specific answers related to the potential employee's ethical standards (Vrij et al., 2014).

Before business owners attempt to prevent asset misappropriation, he or she must have the ability to recognize red flags that are common amongst potential fraudsters, some of which are behavioral ques. Some unusual behavior ques may include refusal to accept new positions, befriending coworkers who are less likely to challenge them, are confrontational and refuse to produce records upon request (Simser, 2014). Prevention of occupational crimes begins with the tone at the top (Elliott et al., 2013). Small business owners should set the tone as well as be the examples of how the business to conduct business activities and what the consequences are for any deviations. Elliott et al., (2013) referred to the organizational climate and culture as the perceptions of organizational practices and procedures that members share among themselves that provide institutionalized normative systems that guide behavior.

Preventative fraud measures transpire prior to the occurrence of any fraudulent act, taking place (Kim & Kogan, 2014). The most effective and common strategies implemented to prevent employee fraud are the use of adequate internal controls that cannot be overridden by management (Hollow, 2014; Kim & Kogan, 2014). Implementation of controls that management cannot override is critical because management is generally responsible for monitoring internal controls and is familiar with how the controls function. Hollow (2014) suggested that some procedures are a separation of duties and improved internal communications. Kim and Kogan (2014) posited that while implementation, development, and maintenance of fraud prevention controls could be costly if implemented promptly, the value would be large enough to justify the cost. The separation of duties is one of the most important internal control mechanisms, as one individual is not performing two conflicting duties such as cash receipts and invoicing (Kitching et al., 2013). Internal controls are imperative for small businesses in preventing asset misappropriation (Rodgers et al., 2015).

Yogi-Prabowo (2014) argued that occupational fraud was widespread and as technology continues to evolve, new methods of conducting business would emerge, and fraudsters would become more clever. Smaller family-owned businesses tend to have weaker internal controls, due to their priority to maintain private benefits according to Bardhan et al. (2015), leaving them more vulnerable to fraud than larger businesses that implement stronger internal controls. The implication for small business owners is that they will have to continue to revisit and revise their internal control strategies to ensure that their policies and procedures remain effective to prevent asset misappropriation. Business owners should incorporate background checks and routine employee training in their business strategies to maintain effective fraud prevention policies (Leistedt & Linkowski, 2016). Gupta et al. (2013) argued that there is no perfect set of internal controls for any industry and that there will always be room for improvements. Additionally, small business owners will be responsible for maintaining a standard of reasonableness and ethics in meeting internal control objectives (Gupta et al., 2013).

Detecting occupational fraud
Fraud prevention measures alone are not sufficient, as it is impossible to implement a fraud prevention system that is entirely failsafe (Kim & Kogan, 2014). There will be internal fraudulent occurrences that bypass the prevention control systems. Whistleblowing has the potential to be the most effective fraud detection mechanism and could possibly end an ongoing fraud scheme such as that at Enron (Gao et al., 2015; MacGregor & Stuebs, 2014). Whistleblowing is one of the most important outlets for reporting organizational fraud according to Ahmad et al. (2014). However, the most effective channels, such as anonymous hotlines

should be available for employees to be able to report fraud without fear of repercussion. Potential whistleblowers have the opportunity to report a fraudulent act that they are aware of as an ethical duty but may not for fear of retaliation from the individual or individuals he or she reported (Gao et al., 2015; MacGregor & Stuebs, 2014).

While whistleblowing is not obligatory, it is strongly encouraged as an internal control mechanism to detect and deter fraudulent organizational activity. Blowing the whistle on colleagues or managers is difficult and burdensome; as such, it would take an individual with strong ethical beliefs, courage, and morals to blow the whistle (M. Zakaria, 2015). Some individuals are concerned with their personal reputation as others may condemn them for whistleblowing; accuse them of disloyalty to their organization by potentially ruining the organization's reputation, and having exposed insider wrongdoing (M. Zakaria, 2015). Contrarily, whistleblowers are also praised for protecting their organization against inside predators that threatened the organization's going concern (M. Zakaria, 2015), thus reinforcing reinforcement that reporting fraudulent activity reflects positively on the organization.

An employee may be reluctant to report fraudulent activity depending on the reporting options. Some organizations offer anonymous and identified reporting or external and face-to-face reporting (Gao et al., 2015; MacGregor & Stuebs, 2014). When face-to-face or internal channels are the only options, it is less likely that employees report fraud. Conversely, when there are external or anonymous options such as hotlines, fraudulent activity is more likely to be reported (Gao et al., 2015). Gao et al. (2015) and MacGregor and Stuebs (2014) posited that seniority of the fraudster had a significant impact on a potential whistleblower's decision to report the crime or continue to stay silent, allowing the fraud to continue. For example, if the perpetrator is a higher level employee, such as a manager, a lower level employee is less likely to report the wrongdoing (Gao et al., 2015; MacGregor & Stuebs, 2014).

Brown et al. (2016) suggested that there are three classifications of whistleblowers: accountants, women, and senior-level management. As examples, Brown et al. referred to the whistleblowers of the Enron and WorldCom accounting frauds, Sherron Watkins and Cynthia Cooper, both women and accountants. As Gao et al. (2015) and MacGregor and Stuebs (2014) suggested, lower level employees are less likely to blow the whistle due to fear of retaliation, loss of the jobs, and damage to their careers, whereas, some women are inherently ethically inclined than men. Despite the imperfections of whistleblowing due in part to the reluctance of some individuals to report fraud, it remains one of the most crucial fraud detection mechanisms (Brown et al., 2016).

Two facts regarding whistleblowing are that whistleblowing systems are mandatory for large organizations in the aftermath significant accounting frauds in the early 2000s and whistleblowing was a tool utilized to detect fraudulent financial reporting (Johansson & Carey, 2016). Johansson and Carey also purported that the fraud triangle provided a framework for their theory on how anonymous reporting channels (ARCs) increased whistleblowing. An ARC encourages whistleblowing because employees can report fraudulent acts such as asset misappropriation anonymously without repercussion (Johansson & Carey (2016). Johansson and Carey argued that because ARCs are mandatory for reporting fraudulent financial reporting, its use extends to other types of frauds such as asset misappropriation as well. Anonymous reporting is key in small businesses; researchers purport that employees report fraud more frequently in smaller businesses than large organizations (Johansson & Carey, 2016). With the use of ARCs, whistleblowing may become a more effect and reliable fraud detection mechanism.

Warren et al. (2015) proposed using big data to detect fraud in accounting; however, the principles apply to any discipline as business owners may generalize each principle. Warren et al. recommended utilizing video data, audio data, and textual data such as email to determine employees perceived motived, perceived rationalizations and perceived opportunities to commit fraud. The elements of the fraud triangle are useful in

analyzing text in emails from disgruntled employees to detect and predict future fraud (Warren et al., 2015). Potential issues with this method of detection lies with overuse, making ethical employees feel uncomfortable with such extensive monitoring. Management should consider whether this method of fraud detection would cause more harm than good. For instance, if employees feel that management is being overly intrusive, they may become less motivated and less productive (Warren et al., 2015).

Method

Data

The purpose of this study was to explore internal control strategies small retail business owners used to prevent and detect employee fraud. Slack et al. (2015) and Yin (2014) stated that the qualitative method is used to explore research questions using multiple data sources including in-depth or semistructured interviews, observations, and documentary evidence. The selection of participants for this study is a source sample where the researcher is required to go to participants businesses to collect firsthand data. Access to participants was initiated through the Small Business Association website and various social media sites where small business owners convene to discuss business best practices and ongoing concerns. A total of six men and women (P1 through P6) small retail business owners were recruited to participate in semistructured interviews regarding how they were able to own and operate their small businesses for more than 5 years, preventing and detecting occupational fraud. Themes were identified using manual and software-assisted techniques.

Methodology and Research Question

The qualitative multiple case study research design was appropriate for this study. Kaczynski et al. (2014) noted that engaging in qualitative research in a credible, high-quality manner requires the researcher to adopt alternative ways of thinking. Researchers conduct qualitative research to explore the number of occurrences of an event or measure the magnitude of an effect (Shelton et al., 2014).

To gain a holistic understanding of the participants' strategies to prevent and detect occupational fraud in their businesses, a minimal number of semistructured questions were asked. To eliminate biases and directional tone from the questions, open-ended questions were asked that allowed each participant to answer freely and willingly. To maintain confidentiality, no questions were asked that would reveal legal matters or personal information. The following questions were asked:

- What internal control strategies do small businesses owners use to prevent and detect employee fraud?
- How did employee fraud affect business operations?
- What internal control strategies allow you to prevent and detect employee fraud?
- What assistance did you require to determine strategies to implement to prevent and detect employee fraud in your business?
- How did you address the key obstacles to implementing your business' strategies for internal controls to prevent and detect employee fraud?
- How do you monitor the effectiveness of internal control strategies to prevent and detect employee fraud?
- What additional information can you provide regarding strategies to prevent and detect employee fraud?

Analyzing and Interpreting the Data

We conducted face-to-face semistructured interviews with six small retail business owners at their places of business as the primary source of data collection pertaining to prevention and detection strategies. Additionally, we observed participants in their work environments, how they interacted with employees, and collected documentation as supplementary support. Observations of the participants validated the internal control strategies each participant reported that they implemented. Examples include adequate lighting on the work floor that made visual monitoring clear whether through video recording or self-monitoring by the business owner. As an additional control mechanism, participants would routinely complete point-of-sale (POS) transactions alongside or instead of their employees to ensure that sales were completed properly.

Other actions participants took to ensure the merchandise count was accurate was to stock the shelves or racks themselves in addition to electronically monitoring inventory. This form of inventory tracking was performed using computer software specific to the business. Participants were also very vigilant of employee movements, even when employees were not in their direct view. Some used mobile devices with live feeds for surveillance cameras on the work floor, while others viewed monitors in a space away from the work floor, where surveillance cameras were recording. Participants also offered documents such as memoranda or general rules for performance in the workplace regarding safety and internal controls.

Employing thematic analysis, the process of interpreting qualitative data and finding patterns, allowed us to create themes based on the data collected from the semistructured interviews and observations. Using thematic analysis provided a structured approach for me to determine the themes most relevant to this study as well as identify how the themes related to the literature. Identifying key themes throughout the study also allowed me to make connections between my findings and how they can be practically applied.

The owners of small retail businesses were affected by employee fraud and what internal strategies were effective in preventing and detecting future instances of employee fraud. The most significant impact that affected business owners was the financial impact. The aftermath of these fraud instances compelled participants to implement internal control strategies to safeguard their businesses from ongoing instances of employee fraud. A consensus among participants is that various forms of employee monitoring and communication are effective strategies to prevent and detect fraud. Frequent inventory tracking by the participants is also a significantly effective strategy to prevent and detect employee fraud as this allows owners to keep a more efficient count of merchandise incoming and outgoing.

Findings

Several codes and themes were developed during the data collection phase of this research. Six themes emerged from the data collection process: (a) financial impact, (b) transaction responsibility and monitoring, (c) networking and business models, (d) communication, (e) separation of duties, and (f) training. NVivo 12 was used to organize, transcribe, code, create themes and develop concepts for my data collection.

Themes Related to the Overarching Research Question

> *Research question:* What internal control strategies do small businesses owners use to prevent and detect employee fraud?

Financial impact
Participants did lacked knowledge of the possible financial impact occupation fraud could have on their businesses prior to implementing effective internal control strategies. Participants expressed their experiences with financial woes due to fraudulent activity of previous employees, with some experiencing more serious

financial hardship than others. The financial impact of the businesses ranged from costs to restaff, loss of inventory, and implementing effective strategies to prevent future instances of fraud. In instances where inventory was tampered with, participants suffered initial loss of profits, especially in terms of seasonal merchandise, as well as subsequent financial burdens when replacing inventory. Respondents also included examples of instances where they were not able to recover from loss of cash, due to improper transactions, but also how they were able to recover from other instances of employee fraud such as loss of merchandise and the actions they took to prevent further instances.

Monitoring and transaction responsibility
Data collected during this study resulted in the findings of multiple strategies the participants implemented to prevent and detect employee fraud. Schnatterly et al. (2018) took a comprehensive approach to reviewing the components of the fraud triangle in relation to how the elements corresponded with employee compensation, company structure, and monitoring. Monitoring is among the key strategies' participants implemented to prevent and detect employee fraud. As implied by Sandhu (2016), the absence or presence of fraud can be assessed by close scrutiny of human behavior that can help identify employees with the propensity to commit fraud.

After experiencing the impact of employee fraud, P1 began training employees to monitor one another while in the workspace. P1 made the decision to monitor employees from afar as not to make anyone feel uncomfortable, but also made it known that each employee would be held accountable for one another, stating, "I trained my employees to monitor each other, to be responsible for one another and I made sure everyone knew they were being monitored and the monitors were responsible for any losses."

P2 implemented the use of cameras throughout the workplace that allowed for a live feed to a mobile device in the event the participant was away from the workplace. P2 also required employees to use employee IDs to monitor each transaction any employee made. Another layer of monitoring P2 implemented was recording of each register transaction separate from the monitoring of employee ID activity. P2 responded, "I had cameras installed in the store that feed directly to my cell phone so I can always see what is going on even when I am not there. I also get alerts if something happens."

P3 implemented the use of employee IDs to monitor employee activity as well. There are also cameras on the premises of P3's business:

> Many in the network that I am a member of began using employee ID to track their transactions as well as the times employees checked in and clocked out. I thought that was a great idea, so we implemented employee IDs also and they have helped a lot, they even track transactions on the business credit card.

P4 through P6 implemented forms of visual monitoring by being present on the workplace floor themselves, remaining vigilant of employee activity.

Kennedy (2017) argued two key points regarding employee fraud; that small business owners should increase use of surveillance cameras and that deterrence using peer influence to increase fraud detection will decrease motivation. The process of employing multiple forms of monitoring allowed the participants to visually process movements of employees that helped determine whether adjustments needed to be made to workplace policy, employee training, or more clear communication. Participants also stated that after implementation of monitoring strategies, employee fraud was eliminated or significantly decreased.

Warren et al. (2015) suggested the use of technology to monitor employees, examples were video, audio, and textual data monitoring. While some participants felt it intrusive on their employees to impose audio

monitoring or textual monitoring, the participants did employ visual and transactional monitoring devices. Video monitoring, POS transaction recording, requiring employees to input an identifying employee number for each transaction, and visual monitoring by the owners were effective controls for the participants. Thus, extending existing literature pertaining to monitoring to prevent and detect fraud in small retail businesses.

Business models and networking

Participants stated multiple resources utilized to assist occupational fraud. Among the most prevalent were networking with other small retail business owners who implemented successful strategies to prevent occupational fraud and the use of small business models. While networking has been useful for decades in business strategy, researchers have focused on larger networking sources. For example, Balleisen (2017) postulated that the Better Business Bureau (BBB) was initially formed by a group of volunteers whose mission was to implement strategies to prevent deceptive marketing practices. Balleisen maintained that the members banned together to raise funds to develop anti-fraud policies.

Like the small network that is now the BBB, some participants in this study are members of networks of small business owners who work together to share strategies on fraud prevention, business trends, and marketing. P2 learned of new surveillance strategies through networking with other boutique owners. P3 regularly networks with approximately 40 other small business owners who have all implemented employee ID systems to monitor employee transactions, which decreases the likelihood for opportunity to commit fraud. P6 is also a member of a small business network where best practices are regularly discussed.

Further, participants shared that they utilized business models to implemented fraud prevention strategies. P1 and P4 obtained business degrees, continued education, gained knowledge of their demographic that allowed them to create their own business models as they pertained to the specific business. P1 stated, "I developed a business model that included frequent inventory control and use of barcoding systems to keep a more accurate count; to deter pilfering." P4 stated, "I developed my own business model through what I learned when I got my degree in small business entrepreneurship and what I learn as I continue to read and learn about the industry." P3, P5, and P6 adopted small business models shared within their networking forums. The commonality between all participants is that with the assistance of business models and support of networks, each participant was able to significantly reduce the opportunity for employees to commit fraud. Peltier-Rivest (2018) argued that an effective anti-fraud model consists of a positive work environment, assistance to help employees resolve personal and work issues, as well as antifraud training.

While networking has provided support for small business owners for decades, the dynamic of networking has changed. Business owners who participated in this study revealed that they participate in networking groups specifically within their line of business, not in the general sense compared to those who began the BBB. With tailored networking groups, small retail business owners were able to exchange ideas and protocols specific to fit their business that lead to strategies to combat employee fraud in their industry. Once such measure was using small retail business models to determine what the overall structures were and how they could use those models to implement controls to protect their business. These measures were found to be most useful during the decision-making process and could be an integral addition to fraud prevention measures going forward. The findings serve as an extension to existing literature on the use of networking as a strategy as well as extending it by offering insight on how small business specific networks can add value to similar businesses.

Communication

Communication and separation of duties were two additional measures participants found effective in preventing and detecting employee fraud. Participants in this study cited communication as an effective strategy when addressing obstacles to implementing internal controls. Several authors have recognized communication as key in reaching employees to express the consequences of committing fraud. K. M. Zakaria

et al. (2016) postulated that communication ensures that relevant and pertinent information is shared throughout the company. Participants stated that in addition to implementing new policies and transaction monitoring procedures, communication was vital in helping employees understand the new processes and allowed them to voice any concerns.

Separation of duties

Most participants in this study experienced employee fraud prior to implementing internal control strategies to prevent and detect future instances of fraud. As one of an array of internal control measures, separation of duties was a vital internal control. With insufficient separation of duties, small business owners cannot detect fraud, thus creating a weak internal control environment, and enabling employee fraud (Akkeren & Buckby, 2017). Kitching et al. (2013) argued that separation of duties was one of the most important internal controls to implement. Moreover, Hollow (2014) suggested that separation of duties and improved communication between owners and their employees were key strategies. These findings add to the validity of assertions made by previous researchers in that participants enforcing control measures were able to decrease or eliminate employee fraud.

P1 discovered the need for separation of duties after experiencing employee fraud, as such, P1 implemented and maintained quarterly inventory control measures that were inventory on hand was compared to employee sales activity in efforts to detect and prevent any inventory loss. P2 began ordering, counting, and auditing inventory while employees completed transactions and maintained the boutique area. In the same manner, P4 separated the duties of employees by limiting employees to maintaining the workspace and completing transactions. Inventory management including ordering, stocking, and retrieval was conducted by the participant. P5 stated, "I count the inventory myself and order products because that shouldn't be a responsibility of my employees." P6 conducts a weekly electronic inventory review comparing sales to inventory on hand to ensure accurate employee sales transactions. P6 also stated that all transactions are process through the POS portal with no exceptions so that each sale item could be accounted for when scanned. This the electronic scanning of products automatically updated product count to reflect accurate levels, made possible because inventory is also tracked and monitored through the same POS portal. P6 physically counts all inventory on an annual basis, but the POS tracking system produces a daily product list that is reviewed daily to determine what items should be restocked. Each participant has benefitted from separating duties, specifically separating the responsibility of inventory and completion of sales transactions. As argued by Akkeren and Buckby (2017), separation of duties provided a strengthened internal control environment, preventing and detecting fraud.

Employee Training

Employee training was a fraud prevention method that participants found effective as continued training served as constant reminders of work ethic, new procedures, and employee expectations. The training aspect would extend existing literature on fraud prevention in small businesses as previous researchers did not cite training as a critical element. However, participants in this study found exceptional value in ongoing employee training. Results provided by participants of this study revealed that ongoing employee training is critical in maintaining ethical standards, understanding of software updates as they pertain to employee use, and expected behavior. Participants emphasized that training is a key element for new and existing employees. P4 and P6 as business owners continue small business trainings to remain abreast of new trends or threats that could potentially affect business operations. The training for P4 and P6 equip these individuals with knowledge that can be shared with employees or utilized to create relatable training material. Robinson and Jonker (2017) explained that training assists employees when facing ethical dilemmas.

Preventing situations where ethics are called into question is a goal each participant strives to accomplish. P1 stated,

anyone engaging in retail should be aware of the potential threats. Others should be aware of their demographic and tailor their training accordingly. I train my employees differently that large retail clothing businesses would since boutiques are vastly different. Boutiques also have a separate inventory experience than larger retail business, some have little to no inventory.

P3 stated, "because of growth processes, and adaptation to constant retail industry changes, continuous training is necessary for our success." P4 stated that "training is necessary for us to continue to be successful." P5 stated, "since cameras a more intrusive, I prefer communication, visual monitoring, and periodic training to maintain a level of trust with my employees." P6 stated, "I provide employees with a handbook and rely on continuous training on work floor etiquette as well as functions like creating purchase orders. Continuous training and open communication are key in preventing fraud for my business."

The findings of this research study confirmed the basis for the conceptual framework, literature review, and overarching research question. The research findings indicated how the fraud triangle could be used as a risk assessment tool as well as a tool to develop strategies to prevent and detect occupational fraud. Participants in this study implemented strategies such as interviewing to help determine if a potential employee's views on ethics fit the business, monitoring prevented and deterred motivation to commit fraud, and employee-to-employee accountability removed the rationalization element.

Because employees in some instances were responsible for and held accountable for each other's actions, it became much more difficult for an employee to commit fraud and rationalize the act. The literature review provided viable information from previous research studies on how internal control strategies similar to those implemented in some larger organizations could be successful in small businesses as well. Participants in this study confirmed that the strategies implemented in their small businesses were transferable across industries and business of any size.

The findings coincide with the fraud triangle theory in that Cressey (1953) suggested that opportunities such as weak internal controls motivate fraudulent acts (K. M. Zakaria et al., 2016). Small retail business owners who voluntarily participated in this study implemented internal control strategies to prevent and detect employee fraud based on the elements of the fraud triangle by understanding (a) pressures, (b) motivations, and (c) rationalizations of perpetrators. As these strategies will be discussed later, participants stated they were vigilant of the change in clientele when certain employees were on duty, an indication of pressure and motivation, and learned from experiences with employee fraud, an indication of rationalizations.

The results of the study revealed that weak internal controls identified by the participants could result in occupational fraud. Some participants relied on interviews to collect information on potential employees, a strategy that Vrij et al. (2014) argued would provide an indication of an individuals' ethical standards. Other participants relied heavily on visual and electronic monitoring to determine an individuals' motivations and rationalizations. Simser (2014) argued that unusual behavior ques could raise red flags regarding an individual's intent to engage in fraudulent activity.

Responses from the semistructured interviews allowed me to identify multiple themes, with six emergent themes being identified as strategies owners of small businesses could implement to prevent and detect employee fraud. Sow et al. (2018) argued that occupational/employee fraud includes asset misappropriation, that is, misuse or theft of cash and inventory. Sow et al. purported that the fraud triangle framework is a key factor in preventing and detecting occupational fraud.

Discussion

Implications

The findings from this study could benefit small retail business owners by introducing strategies that small business owners could implement to prevent and detect employee fraud. The results from this study provide insight on how the participants of this study created and implemented strategies to safeguard their businesses against employee fraud, which can be useful in other small retail businesses. The findings from this study could provide other small retail business owners with insight on the importance of training their employees to prevent fraud, a strategy that was most helpful to each participant in this study.

Implementing effective internal control strategies to protect small business assets affords owners the opportunities to flourish within the community by increasing employment opportunities, increasing income distribution, and decreasing social conflict. Placing an emphasis on social entrepreneurship, small business owners serve their communities by focusing on wealth distribution, addressing issues of hunger, education, and unemployment (Lumpkin et al., 2013). Employment creation and economic stability have positive effects on society. For small business owners to secure their businesses within their communities a sound internal control structure is necessary.

Conclusion

The main issue is that some small retail business owners lack strategies to implement internal controls to prevent and detect employee fraud. The purpose of this qualitative multi case study was to explore internal control strategies small retail business owners use to prevent and detect employee fraud. The findings of this study revealed strategies small retail business owners could implement to protect their businesses from employee fraud including (a) video monitoring, (b) employee IDs to track employee activity, (c) separation of duties, and (d) effective communication with employees. Frequent inventory tracking by the participants is also a significantly effective strategy to prevent and detect employee fraud as this allows owners to keep a more efficient count of merchandise incoming and outgoing.

Employee fraud is a serious issue in small business as fraud causes interruption of business operations, costs business owners additional time and resources to reverse the damage caused by fraud, and could tarnish business reputation (Omar et al., 2016). The results of this study may be useful to small retail business owners who need to implement effective internal control strategies to prevent employee fraud. Moreover, results from this study could provide guidance for current and aspiring small retail business owners in understanding the significance of implementing and maintaining internal control strategies.

References

Ahmad, S. A., Yunos, R. M., Raja-Ahmad, R. A., & Sanusi, Z. M. (2014). Whistleblowing behavior: The influence of ethical climates theory. *Procedia-Social Sciences and Behavioral Sciences, 164,* 445–450. https://doi.org/10.1016/j.sbspro.2014.11.101

Akkeren, J., & Buckby, S. (2017). Perceptions on the causes of individual and fraudulent c0-offending: Views of forensic accountants. *Journal of Business Ethics, 146,* 383–404. https://doi.org/10.1007/s10551-015-2881-0

Alleyne, B., & Amaria, P. (2013). The effectiveness of corporate culture, auditor education, and legislation in identifying, preventing, and eliminating corporate fraud. *International Journal of Business, Accounting, and Finance, 7,* 34–62.

Anand, V., Dacin, M. T., & Murphy, P. R. (2015). The continued need for diversity in fraud research. *Journal of Business Ethics, 131,* 751–755. https://doi.org/10.1007/s10551-014-2494-z

Andon, P., Free, C., & Scard, B. (2015). Pathways to accountant fraud: Australian evidence and analysis. *Accounting Research Journal, 28,* 10–44. https://doi.org/10.1108/ARJ-06-2014-0058

Azim, M. I., & Azam, S. (2016). Bernard Madoff's "Ponzi Scheme": Fraudulent behavior and the role of auditors. *Accountancy Business and the Public Interest, 15,* 122–137.

Azizul-Islam, M. (2014). Bribery and corruption in Australian local councils. *Public Money & Management, 34,* 441–446. https://doi.org/10.1080/09540962.2014.962372

Bakri, H. H. M., Mohamed, M., & Said, J. (2017). Mitigating asset misappropriation through integrity and fraud frisk elements: Evidence emerging economies. *Journal of Financial Crime, 24,* 242–255. https://doi.org/10.1108/JFC-04-2016-0024

Balleisen, E. J. (2017). American better business bureaus, the truth-in-advertising movement, and the complexities of legitimizing business self-regulation over the long term. *Politics and Governance, 5,* 42–43. https://doi.org/10.17645/pag.v5i1.790

Bardhan, I., Lin, S., & Wu, S. L. (2015). The quality of internal control over financial reporting in family firms. *American Accounting Association, 29,* 41–60. https://doi.org/10.2308/acch-50935

Bhasin, M. (2013). Corporate governance and forensic accountant: An exploratory study. *Journal of Accounting–Business & Management, 20*, 55–83.

Bonny, P., Goode, S., & Lacey, D. (2015). Revisiting employee fraud: Gender, investigation outcomes and offender motivation. *Journal of Financial Crime, 22,* 447–467. https://doi.org/10.1108/JFC-04-2014-0018

Boyle, D. M., Boyle, J., & Mahoney, D. (2015). Avoiding the fraud mindset. *Strategic Finance, 97*(2), 41–46.

Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy, 34,* 578–596. https://doi.org/10.1016/j.jaccpubpol.2015.05.006

Brown, J. O., Hays, J., & Stuebs, M. T. (2016). Modeling accountant whistleblowing intentions: Applying the theory of planned behavior and the fraud triangle. *Accounting and the Public Interest, 16,* 28–56. https://doi.org/10.2308/apin-51675

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*, 36–54. https://doi.org/10.1057/sj.2012.11

Clor-Proell, S., Kaplan, S., & Proell, C. (2015). The impact of budget goal difficulty and promotion availability on employee fraud. *Journal of Business Ethics, 131,* 773–790. https://doi.org/1007/s1051-013-2021-7

Cressey, D. R. (1953). *Other people's money: A study of the psychology of embezzlement*. Free Press.

Daigle, R. J., Hayes, D. C., & Morris, P. W. (2014). Dr. Phil and Montel help AIS students "get real" with the fraud triangle. *Journal of Accounting Education, 32,* 146–159. https://doi.org/10.1016/j.jaccedu.2014.03.004

Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum, 37,* 29–39. https://doi.org/10.1016/j.accfor.2012.09.003

Dhamija, S. (2014). Whistleblower policy-time to make it mandatory. *Global Business Review, 15,* 833–846. https://doi.org/10.1177/0972150914535142

Ding, S., & Wu, Z. (2014). Family ownership and corporate misconduct in U.S. small firms. *Journal of Business Ethics, 123,* 183–195. https://doi.org/10.1007/s10551-013-1812-1

Eaton, T. V., & Korach, S. (2016). A criminological profile of white-collar crime. *The Journal of Applied Business Research, 32,* 129–142.

Elliott, T. L., Marquis, L. M., & Neal, C. S. (2013). Business ethics perspectives: Faculty plagiarism and fraud. *Journal of Business Ethics, 112,* 91–99. https://doi.org/10.1007/s10551-012-1234-5

Favere-Marchesi, M. (2013). Effects of decomposition and categorization on fraud-risk assessments. *Auditing: A Journal of Practice & Theory, 32,* 201–219. https://doi.org/10.2308/ajpt-50528

Feldman, M. P. (2014). The character of innovative place: Entrepreneurial strategy, economic development, and prosperity. *Small Business Economics, 43,* 9–20. https://doi.org/10.1007/s11187-014-9574-4

Finnerty, J. D., Hegde, S., & Malone, C. B. (2016). Fraud and firm performance: Keeping the good times (apparently) rolling. *Managerial Finance, 42,* 151–172. https://doi.org/10.1108/MF-01-2015-0009

Fortvingler, J., & Szívós, L. (2016). Different approaches to fraud risk assessment and their implications on audit planning. *Periodica Polytechnica Social and Management Sciences, 24,* 102–112. https://doi.org/10.3311/PPso.8436

Gao, J., Greenberg, R., & Wong-On-Wing, B. (2015). Whistleblowing intensions of lower-level employees: The effect of reporting channel, bystanders, and wrongdoer power status. *Journal of Business Ethics, 126,* 85–99. https://doi.org/10.1007/s10551-013-2008-4

Gilmore-Allen, A. (2015). Tech fraud and the small business. *Internal Auditor, 72,* 20–21.

Goldstein, D. (2015). Occupational fraud: Misappropriation of assets by an employee. *Journal of the International Academy for Case Studies, 21,* 81–86.

Graham, W. J., & Cooper, W. H. (2013). Taking credit. *Journal of Business Ethics, 115,* 403–425. https://doi.org/10.1007/s10551-012-1406-3

Gullkvist, B., & Jokipii, A. (2013). Perceived importance of red flags across fraud types. *Critical Perspectives on Accounting, 24,* 44–61. https://doi.org/10.1016/j.cpa.2012.01.004

Gupta, P., Weirich, T., & Turner, L. (2013). Sarbanes-Oxley and public reporting on internal control: Hasty reaction or delayed reaction? *Accounting Horizons, 27,* 371–408. https://doi.org/10.2308/acch-50425

Hamilton, E. L. (2016). Evaluating the intentionality of identified misstatements: How perspective can help auditors in distinguishing errors from fraud. *Auditing Journal of Practice & Theory, 35,* 57–78. https://doi.org/10.2308/ajpt-51452

Henry, L. (2016, April). Fraud prevention. *Internal Auditor, 73*(2), 17–19. http://www.theiia.org/ecm/magazine.cfm?doc_id=540

Hollow, M. (2014). Money, morals and motives: An exploratory study into why bank managers and employees commit fraud at work. *Journal of Financial Crime, 21,* 174–190. https://doi.org/10.1108/JFC-02-2013-0010

Holtfreter, K. (2015). General theory, gender-specific theory, and white-collar crime. *Journal of Financial Crime, 22,* 422–431. https://doi.org/10.1108/JFC-12-2014-0062

Hunt, G. L., & Austin, S. F. (2014). A descriptive comparison of two sources of occupational fraud data. *Journal of Business & Economics Research, 12,* 171–176.

Ishida, C., Chang, W., & Taylor, S. (2016). Moral intensity, moral awareness and ethical predispositions: The case of insurance fraud. *Journal of Financial Services Marketing, 21,* 4–18. https://doi.org/10.1057/fsm.2015.26

Johansson, E., & Carey, P. (2016). Detecting fraud: The role of the anonymous reporting channel. *Journal of Business Ethics, 139,* 391–409. https://doi.org/10.1007/s10551-015-2673-6

Kaczynski, D., Salmona, M., & Smith, T. (2014). Qualitative research in finance. *Australian School of Business, 39,* 127–135. https://doi.org/10.1188/0312896212469611

Kennedy, J. P. (2016). Sharing the keys to the kingdom: Responding to employee theft by empowering employees to be guardians, place managers, and handlers. *Journal of Crime and Justice, 39,* 512–527. https://doi.org/10.1080/0735648X.2014.998701

Kennedy, J. P. (2017). Functional redundancy as a response to employee theft within small businesses. *Security Journal, 30*, 162–183. https://doi.org/10.1057/sj.2015.37

Kim, Y., & Kogan, A. (2014). Development of an anomaly detection model for a bank's transitory account system. *Journal of Information Systems, 28,* 145–165. https://doi.org/10.2308/isys-50699

Kitching, K. A., Pevzner, M., & Stephens, N. M. (2013). Comments by the auditing standards committee of the auditing section of the American accounting association on the COSO request for comment on internal control over external financial reporting: Compendium of approaches and examples. *Current Issues in Auditing, 7*(1), C30–C33. https://doi.org/10.2308/ciia-50475

Klein, R. (2015). How to avoid or minimize fraud exposures. *CPA Journal, 85*(3), 6–8.

Krambia-Kapardis, M., & Papastergiou, K. (2016). Fraud victimization in Greece: Room for improvement in prevention and detection. *Journal of Financial Crime, 23,* 481–500. https://doi.org/10.1109/JFC-02-2015-0010

Kramer, B. (2015). Trust but verify fraud in small businesses. *Journal of Small Business and Enterprise Development, 22,* 4–20. https://doi.org/10.1108/JSBED-08-2012-0097

Kummer, T. F., Singh, K., & Best, P. (2015). The effectiveness of fraud detection instruments in not-for-profit organizations. *Managerial Auditing Journal, 30,* 435–455. https://doi.org/10.1108/MAJ-08-JFC-09-2015-0053

Lail, B., MacGregor, J., Marcum, J., & Stuebs, M. (2017). Virtuous professionalism in accountants to avoid fraud and to restore financial reporting. *Journal of Business Ethics, 140,* 687–704. https://doi.org/10.1007/s10551-015-2875-y

LaSalle, R. E. (2007). Effects of the fraud triangle on students' risk assessment. *Journal of Accounting Education, 25,* 74–87. https://doi.org/10.1016/j.jaccedu.2007.03.002

Leistedt, S. J., & Linkowski, P. (2016). Fraud, individuals, and networks: A biopsychosocial model of scientific frauds. *Science and Justice, 56,* 109–112. https://doi.org/10.1016/j.scijus.2016.01.002

Lenz, P. J., & Graycar, A. (2016). Stealing from the boss: Who is looking? *Journal of Financial Crime, 23,* 613. https://doi.org/10.1108/JFC-09-2015-0053

Lightle, S. S., Baker, B., & Castellano, J. F. (2015). Assessment of tone at the top: The psychology of control risk assessment. *The CPA Journal, 85,* 50–55.

Lin, C. C., Chiu, A. A., Huang, S. Y., & Yen, D. C. (2015). Detecting the financial statement fraud: The analysis of the differences between data mining techniques and experts' judgments. *Knowledge-Based Systems, 89,* 459–470. https://doi.org/10.1016/j.knosys.2015.08.011

Liu, X. K., Wright, A. M., & Wu, Y. J. (2015). Managers' unethical fraudulent financial reporting: The effect of control strength and control framing. *Journal of Business Ethics, 129,* 295–310. https://doi.org/10.1007/s10551-014-2156-1

Lofland, C., & McNeal, A. (2014). What's your fraud IQ? *Journal of Accountancy, 217*(3), 46–50.

Lumpkin, G. T., Moss, T. W., Gras, D. M., Kato, S., & Amezcua, A. S. (2013). Entrepreneurial processes in social contexts: How are they different, if at all? *Small Business Economics, 40,* 761–783. https://doi.org/10.1007/s11187-011-9399-3

MacGregor, J., & Stuebs, M. (2014). The silent Samaritan syndrome: Why the whistle remains unblown. *Journal of Business Ethics, 120,* 149–164. https://doi.org/10.1007/s10551-013-1639-9

Manning, L., Smith, R., & Soon, J. M. (2016). Developing an organizational typology of criminals in the meat supply chain. *Food Policy, 59,* 44–54. https://doi.org/10.1016/j.foodpol.2015.12.003

Mihret, D. G. (2014). National culture and fraud risk: Exploratory evidence. *Journal of Financial Reporting and Accounting, 12,* 161–176. https://doi.org/10.1108/JFRA-10-2012-0049

Mishra, S., & Singh, G. (2017). Forensic accounting: An emerging approach to deal with corporate frauds in India. *Global Journal of Enterprise Information System, 9*(2), 104–109. https://doi.org/10.18311/gjeis/2017/15922

Morgan, A. R., & Burnside, C. (2014). Olympus corporation financial statement fraud case study: The role that national culture plays on detecting and deterring fraud. *Journal of Business Case Studies, 10,* 175–181.

Mui, G., & Mailley, J. (2015). A tale of two triangles: Comparing the fraud triangle with criminology's crime triangle. *Accounting Research Journal, 28,* 45–58. https://doi.org/10.1108/ARJ-10-2014-0092

Omar, M., Nawawi, A., & Salin, A. S. A. P. (2016). The causes, impact and prevention of employee fraud. *Journal of Financial Crime, 23*, 1012–1027. https://doi.org/10.1108/JFC-042015-0020

Peltier-Rivest, D. (2018). A model for preventing corruption. *Journal of Financial Crime, 25,* 545–561. https://doi.org/10.1108/JFC-11-2014-0048

Peltier-Rivest, D., & Lanoue, N. (2015). Cutting fraud losses in Canadian organizations. *Journal of Financial Crime, 22,* 295–304. https://doi.org/10.11/08/JFC-11-2013-0064

Peters, S., & Maniam, B. (2016). Corporate fraud and employee theft: Impacts and costs on business. *Journal of Business & Behavioral Sciences, 28,* 104–117.

Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance, 16*, 489–497. https://doi.org/10.1016/s2212-5671(14)00829-6

Pierce, L., & Snyder, J. (2015). Unethical demand and employee turnover. *Journal of Business Ethics, 131,* 853–869. https://doi.org/10.1007/s10551-013-2018-2

Power, M. (2013). The apparatus of fraud. *Accounting, Organizations, and Society, 38,* 525–543. https://doi.org/10.1016/j.aos.2012.07.004

Robinson, B. M., & Jonker, J. A. (2017). Inculcating ethics in small and medium sized business enterprises: A South African leadership perspective. *African Journal of Business Ethics, 11*(1), 63–81. https://doi.org/10.15249/11-1-132

Rodgers, W., Soderbom, A., & Guiral, A. (2015). Corporate social responsibility enhanced control systems reducing the likelihood of fraud. *Journal of Business Ethics, 131,* 871–882. https://doi.org/10.1007/s10551-014-2152-5

Sandhu, N. (2016). Behavioural red flags of fraud – A qualitative assessment. *Journal of Human Values, 22,* 221–237. https://doi.org/10.1177/0971685816650579

Schnader, A. L., Bedard, J. C., & Cannon, N. (2015). The principal-agent dilemma: Reframing the auditor's role using stakeholder theory. *Accounting and the Public Interest, 15*, 22–26. https://doi.org/10.2308/apin-51234

Schnatterly, K., Gangloff, K. A., & Tuschke, A. (2018). CEO wrongdoing: A review of pressure, opportunity, and rationalization. *Journal of Management, 44,* 2405–2432. https://doi.org/10.1177/0149206318771177

Shelton, C. L., Smith, A. F., & Mort, M. (2014). Opening up the black box: An introduction to qualitative research methods in anesthesia. *Anesthesia, 69,* 270–280. https://doi.org/10.1111/anae.12517

Sídoróv, J. (2015). Best practices for health outcomes public reporting. *Population Health Management, 18,* 399-401. https://doi.org/10.1089/pop.2015.0033

Simser, J. (2014). Culpable insiders-the enemy within, the victim without. *Journal of Financial Crime, 21,* 310–320. https://doi.org/10.1108/JFC-11-2013-0068

Slack, R. E., Corlett, S., & Morris, R. (2015). Exploring employee engagement with (corporate) social responsibility: A social exchange perspective on organizational participation. *Journal of Business Ethics, 127*, 537–548. https://doi.org/10.1007/s10551-014-2057-3

Small Business Development Center (SBDC). (2017). *Small business in Pennsylvania*. Retrieved from http://www.pasbdc.org/resources/small-biz-stats

Smith, R. (2016). Of bad seed, black-sheep and prodigal-sons: Profiling crime and enterprise in a small-business-community. *International Journal of Entrepreneurial Behavior & Research, 22,* 39–62. https://doi.org/10.1108/IJEBR-04-2014-0059

Sorunke, O. A. (2016). Personal ethics and fraudster motivation: The missing link in fraud triangle and fraud diamond theories. *International Journal of Academic Research in Business and Social Sciences, 6,* 159–165. https://doi.org/10.6007/IJARBSS/v6-i2/2020

Sow, A. N., Basiruddin, R., Rasid, S. Z. A., & Husin, M. M. (2018). Understanding fraud in Malaysian SMEs. *Journal of Financial Crime, 3,* 870–881. https://doi.org/10.1108/JFC-08-2017-0077

Stone, D. M. (2015). Post-Hunton: Reclaiming our integrity and literature. *Journal of Information Systems, 29,* 211–227. https://doi.org/10.2308/isys-51094

Suliman, S., Danbatta, B. L., & Rahman, R. A. (2014). Figure massaging practices in Malaysian firms: Are they fraudulent? *Procedia–Social and Behavioral Sciences, 145,* 29–39. https://doi.org/10.1016/m.sbspro.2014-06-008S

Tsegba, I. N., & Upaa, J. U. (2015). Consequences of financial statement fraud: A developing country perspective. *International Journal of Business and Management, 10,* 115–126. https://doi.org/10.5539/ijbm.v10n8p115

Van Gelder, J. L., & DeVries, R. E. (2016). Traits and states at work: Lure, risk, and personality as predictors of occupational crime. *Psychology, Crime & Law, 22,* 701–720. https://doi.org/10.1080/1068316X.2016.1174863

Vrij, A., Hope, L., & Fisher, R. P. (2014). Eliciting reliable information in investigative interviews. *Policy Insights from the Behavioral and Brain Sciences, 1,* 129–136. https://doi.org/10.1177/2372732214548592

Warren, J. D., Moffitt, K. C., & Byrnes, P. (2015). How big data will change accounting. *Accounting Horizons, 29,* 397–407. https://doi.org/10.2308/acch-51069

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Sage.

Yogi-Prabowo, H. (2014). To be corrupt or not to be corrupt: Understanding the behavioral side of corruption in Indonesia. *Journal of Money Laundering Control, 17,* 306–326. https://doi.org/10.1108/JMLC-11-2013-0045

Zakaria, K. M., Nawai, A., & Salin, A. S. A. P. (2016). Internal controls and fraud-empirical evidence from oil and gas company. *Journal of Financial Crime, 23,* 1154–1168. https://doi.org/10.1108/JFC-04-2016-0021

Zakaria, M. (2015). Antecedent factors of whistleblowing in organizations. *Procedia Economics and Finance, 28,* 230–234. https://doi.org/10.1016/S2212-5671(15)01104-1