Journal of Management Control (2022) 33:189–213
https://doi.org/10.1007/s00187-022-00335-w

ORIGINAL PAPER

In employees we Trust: Employee fraud in small businesses

Radiah Othman[1] · **Rashid Ameer**[2]

Accepted: 19 January 2022 / Published online: 5 April 2022

Abstract

This paper examines how and why employees used online computer access to commit fraud in New Zealand small businesses. Drawing on data from 18 court documents between 2006 and 2020, we use document analysis to examine the pressure, opportunity, rationalization, and capability elements using the fraud diamond framework. We provide three major findings. First, the employee frauds were motivated by vice and family circumstances. The combination of opportunity and capability had a devastating effect on the length of the fraud and the amount of financial loss. Second, the frauds were mostly perpetrated by middle-aged women in both managerial and nonmanagerial positions who displayed unusual behaviour but had no prior convictions. Third, small businesses are vulnerable to fraud in their billing, accounts payable, and payroll systems; thus, relevant prevention strategies are recommended. Overall, we conclude that the tendency for fraud is heightened in small businesses where trusted employees: have multiple responsibilities; have an occupational position that provides them with opportunity; are capable of manipulating online access; and have external pressures of addictions or adverse family circumstances. Our multiple cases approach facilitates a better understanding of the employee fraud contexts, including the motivation and the methods employed to commit such fraud in New Zealand.

Keywords Employee fraud · Online computer access · Internal control · Management control · Small business · Prevention strategies · New Zealand

Classification Code M40

✉ Radiah Othman
r.othman@massey.ac.nz

[1] Business Studies West 3.16, School of Accountancy, Massey Business School, Private Beg 11222, PN4410 Palmerston North, New Zealand

[2] IPU New Zealand Tertiary Institute, School of Global Studies, Palmerston North, New Zealand

1 Introduction

Small businesses are victimized more regularly than larger businesses and significantly harmed by insiders (ACFE, 2018, 2020; Bunn et al., 2019; PWC, 2018; Kennedy, 2018; Hess & Cottrell Jr., 2016). Employee fraud is the main cause of small business failure and negatively affects the businesses' operations (ACFE, 2020; Bunn et al., 2019; Carland et al., 2001; Feng, 2018; Jackson et al., 2010). The full scale of employee fraud involving small businesses in New Zealand is still unknown (e.g., Hay, 2015; Othman, et al., 2020). The Financial Crime Group (FCG), a branch of the New Zealand Police, has many fraud cases on its books that have remained uninvestigated for years (Gillam, 2018). Scholars have noted that research on fraud in small businesses needs further academic scrutiny (Johnson & Rudesill, 2001; Kramer, 2015). Previous studies are largely dominated by US cases and thus lack global representation (Albrecht et al., 2008). There are approximately 450,000 small businesses in New Zealand which employ nearly one-third of the private sector workforce (MBIE, 2015; NZentrepreneur, 2017). Many aspects of the small business working environment have changed since 2015 as a result of a greater use of technology in New Zealand (Scoop, 2020).

More than 20 years ago, Haugen and Selin (1999) cautioned that businesses were becoming more susceptible to computer crime committed by insider employees. The double-edged sword of the online environment improves small business efficiency but also imbues employees with the intent to commit and conceal fraud (Hess & Cottrell Jr., 2016; Ruankaew, 2016). The literature on online and computer fraud in small businesses has tended to emphasize external threats (e.g., Schaper & Weber 2012; Junger et al., 2020). Widespread use of computers has enabled insider fraudsters to steal from their employers more quickly and in larger amounts. Often, inputs and outputs are altered, and data files are manipulated using unauthorized access or privileges beyond those required to perform assigned job functions due to a lack of duty segregation (Haugen & Selin, 1999; Kranacher et al., 2011, p. 119). These employees use their positions to take or divert assets belonging to their employer as they are aware of the "flaws" in the control system and use them to their advantage (Albrecht et al., 2019; Kranacher et al., 2011, p. 119). As reported by ACFE (2020), one-third of fraudsters conceal their fraud by altering electronic documents or creating fraudulent ones. In essence, computers provide a gateway for fraud, as there are "no outward signs or indicators that anything is amiss" (Haugen & Selin, 1999, p. 342).

Framed by fraud diamond theory, our main research question is how and why employees used online computer access to commit fraud in New Zealand small businesses. In this study, 18 court documents involving employee fraud from 2006 to 2020 were analyzed. Based on the analysis, suitable fraud risk prevention and detection strategies, which may be of interest to investigating authorities and antifraud professionals, are then proposed for business owners and managers. In this study, the terms online access, computer access and online computer access are used interchangeably.

The contributions of this study are fourfold. *First*, this study analyzes employee fraud committed via the use of online computer access in small New Zealand businesses. Previous studies on online and computer fraud in small businesses has tended to emphasize external rather than insider threats (e.g., Schaper & Weber 2012; Junger

et al., 2020). *Second*, insider threats can be devastating to the New Zealand economy as small businesses constitute 97% of the country's enterprises and contribute more than one-quarter of the gross domestic product (MBIE, 2015; NZentrepreneur, 2017). However, the impact of fraud losses is unknown. *Third*, this study examines court documents to provide insights into how employee frauds were perpetrated and into the effects of the fraud on its victims. This highlights the importance of the four-eyes principle as a main prevention strategy. *Last*, this study details the fraud scheme types and actual fraud losses reported by the court documents.

The next section provides a literature review of the extant studies on fraud in small businesses. Section 3 explains the research framework based on fraud diamond theory, which is followed by the methodology used to collect and analyze the data in Sect. 4. Section 5 discusses the findings and discussion of the study, and the last section concludes and provides recommendations for small businesses in mitigating employee fraud.

2 Literature review

Published works on fraud in small business have largely used data from international fraud surveys (e.g., ACFE, 2020). These surveys invite fraud examiners to self-report their most recent completed fraud cases. Most cases are not gauged from the victims' or perpetrators' viewpoints. Moreover, the fraud losses are estimated rather than actual. As a fraudster's demographic and psychological profile cannot be distinguished from an honest person's profile, the knowledge and understanding of *why* an employee commits fraud might help to predict its likelihood. Albrecht et al., (2019, p. 34) suggest that approximately 95% of all frauds involve either financial or vice-related pressure. Hess and Cottrell Jr. (2016, p. 16) assert that small transgressions, if left unchecked, can have a devastating future impact. Indeed, an employee turns to fraud when he or she knows that no one is watching. The assumption that an employee is always honest and able to resist temptation is naïve (Carland et al., 2001). Trusted employees have been widely documented to become insider fraudsters (e.g., Jackson et al., 2010; Hight, 2015), but they are yet to be studied in a small business context.

Fraud symptoms or indicators can assist small business owners to detect fraud. Fraud detection techniques published in the internal auditing literature, such as the Beneish model (Beneish, 1999), the Altman Z-score (Altman, 1968), and Benford's law (Nigrini, 2019; Benford, 1938), are more suitable for detecting financial statement rather than employee fraud. Albrecht et al., (2019) suggest that symptoms such as internal control weaknesses and lifestyle and behavioural symptoms, including employees' past convictions, can provide good indicators of the likelihood of employee fraud. 60% of employee fraud is committed because a business has weak internal controls (KPMG, 2020). Nonetheless, internal and management control systems can never guarantee fraud-free behaviour as employees' temptations and needs change (Merchant & Van der Stede, 2007; Deschamps, 2019). As quoted by Corns (1971, p. viii), "Controls protect weak people from temptation, strong people from opportunity, and innocent people from suspicion". Ignoring controls and allowing

them to be easily overridden by the most trusted employees in the company could jeopardize the longevity of a business and the employment security of the other employees; thus, the consequences of employee fraud could be devastating. However, the non-financial consequences of fraud on small business owners as victims is not widely reported as most of the information can only be derived from victim impact statements in court documents.

Fraud schemes could be perpetrated online and offline. As technology continues to evolve, new methods of conducting business emerge, as do methods of perpetrating fraud (Yogi-Prabowo, 2014). In New Zealand, approximately 33% of small business owners are aged over 55; thus, they did not grow up in the digital age, computers were not part of their schooling, and they have had little opportunity to develop digital skills (Kirkwood & Viitanen, 2015; Digital Inclusion Research Group, 2017). The use of checks for business transactions has largely disappeared, and it is more common for payments to be made by electronic fund transfer (EFT) using online banking platforms. Computers and online platforms have thus become a necessity for business competitiveness, but business owners are often too busy micromanaging their businesses to manage such technology effectively. In many instances, business owners with "obsolete" computerized skills are erroneously convinced that employees with better technological skills are valuable assets and can be trusted, overlooking the importance of the four-eyes principle[1] (Smith, 2016; Othman et al., 2020). Previous studies (e.g., Kramer, 2015) have extracted the fraud schemes from ACFE surveys (e.g., ACFE, 2020) which were pre-determined and not focused on computers or online access environments.

It is critical for business owners to have awareness and knowledge of how to prevent employee fraud in their organizations. Earlier writings in the literature have focused on textbook preventive strategies and were not driven from real life cases that take into consideration the small business context (e.g., Laufer, 2011; Jackson et al., 2010; Alstete, 2006; Cant et al., 2013). They were also analyzed at the aggregate level and might not represent a complete picture on how devastating employee fraud is in small businesses (Kennedy, 2018; Kramer, 2015). Previous studies recommend prevention strategies such as close monitoring and pre-employment screening (Davis, 2019; Omar et al., 2016; Yekini et al., 2018). Focusing on victims of occupational fraud in various industries, Peltier-Rivest (2009) suggest ethics training and anonymous reporting mechanisms for fraud prevention. However, these studies do not investigate employee fraud perpetrated using online computer access and do not consider small businesses as distinct from larger organizations.

In summary, this study bridges the gap in the literature by exploring employee fraud in small businesses, examining the reasons the fraud is committed by (insiders) employees, *how* the fraud was perpetrated (fraud schemes) using online computer access, and other contextual factors such as the fraud symptoms, the actual amount of fraud losses, financial and nonfinancial consequences of the fraud on the victims, based on the narratives of the perpetrator, the victim, and the court, as contained in

[1] Four-eyes principle is a widely used internal control mechanism that requires any action and decision within an organization to be independently verified and approved by a second individual. We would like to credit one of the reviewers who reminded us of this principle.

court case documents. This approach enables us to recommend suitable prevention strategies.

3 Theoretical framework

Perceived need alone will not precipitate fraud. As such, the present study's framework is driven by fraud diamond theory, following Cressey's (1953, p. 30) argument that, "trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property". Cressey's conceptualization of trust violation, known as the fraud triangle (Albrecht et al., 2019; Huber 2017; Free, 2015), has been expanded to include a fourth dimension, capability, and the expanded version is known as the fraud diamond. The fraud diamond framework fits well with the aim of this study, as online computer access and positions of responsibility (managerial and nonmanagerial) represent the prerequisites—opportunity and capability—to commit fraud against their employers. Homer (2020) proposed fifth and sixth elements, but they are more suitable for financial statement fraud contexts. The fifth element, competence, however, is closely related to the fourth element, capability, of the fraud diamond.

The first element of the fraud diamond framework is pressure, which can be financial and nonfinancial, such as low salaries and high credit card debts. It can also be the outcome of feeling undervalued or simply resentful toward the employer (Bunn et al., 2019; Free & Murphy, 2015). While small business owners may be unable to control pressure, they can minimize opportunity, the second element of the fraud diamond framework. Opportunity can be actual or perceived (Albrecht et al., 2019). Small businesses usually employ relatively simple internal controls which provide more opportunities for employees who intend to commit fraud against their employers (KPMG, 2020; Smith et al., 2013; Lofland & McNela, 2014; Gottschalk, 2020a, b). Internal control is generally defined as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" (Committee of Sponsoring Organizations, COSO, 2013). Internal controls are critical to safeguard assets, ensure that financial information is accurate and reliable, and ensure compliance with all financial and operational requirements (Kranacher et al., 2011; Feng, 2018). The internal controls evaluate the effectiveness of management controls; thus, both control systems complement each other. A management control system can influence the way employees behave (Merchant & Van der Stede, 2007). Managers tend to gauge numbers when the control system has flaws and take the first step in appropriating control for their own needs (Deschamps, 2019). According to Cressey (1953), the higher an employee's position in the organization, the higher the level of trust the employer has in that individual. There are thus limitless opportunities for capable but unethical

employees. According to Zarzycka et al., (2019), the ethical environment strongly affects the tendency to engage in questionable behaviour.

The third element is rationalization. An honest employee must be able to rationalize a fraudulent action as acceptable to believe that the action is not criminal, perceiving it as a temporary loan, for example. In this study, rationalization was coded as internal or external. Internal rationalization is internalized self-belief about the deviant behavior as a defense based on necessity or regret about the action. External rationalization is when the perpetrator shifts the responsibility to other people, such as family members and colleagues. Upon discovery of fraud, many small businesses merely dismiss dishonest employees rather than reporting them to the authorities for prosecution. In doing so, they eliminate the problem but inadvertently signal other employees that fraud perpetrators can commit fraud with impunity. When combined with pressure and rationalization, this "perceived opportunity" can result in more fraud in the future when the fraudster moves on to other businesses (Albrecht et al., 2019). The fourth element, capability, in the fraud diamond framework refers to the personal traits and cognitive abilities of fraudsters who occupy authoritative positions in organizations. Wolfe and Hermanson (2004) suggest that fraud can be perpetrated only if fraudsters are capable and skillful. An authoritative position can also determine the type of fraud committed and give the fraudster confidence that it will not be detected (Wolfe & Hermanson, 2004; Holtfreter, 2005; Dorminey et al., 2012). The fraud diamond elements are present in most fraud cases in the sample.

4 Methodology

4.1 Sample

In this study, we used court cases in the New Zealand jurisdiction from the online database of Westlaw NZ, which provides publicly accessible legal information. The search for relevant cases was performed by narrowing it to criminal law offenses involving "computers" and "fraud" for "obtaining by deception", "accessing for dishonest use" and "accessing system without authorization". The cases were reviewed to identify those that specifically mentioned small businesses. The cases were then checked to avoid duplication in the final sample.

Table 1 Years included, number of fraud cases and cases involving small businesses

	Search criteria	Years included	Total no. of cases	Small businesses
1	Computer—Accessing for dishonest purposes	2012-2020	38	5
2	Computer—Accessing system without authorization	2010–2018	3	—
3	Fraud—Obtaining by deception	1912–2021	285	7
4	Fraud—General	1880–2021	1,125	6
	Final sample			18

The final sample based on the search performed on 4 June 2021 is shown below (Table 1). The total number of 18 cases represents fraudsters prosecuted between 2006 and 2020 for fraud in small businesses using online computer access. In Norway, Gottschalk used a single case study to examine occupational crimes (Gottschalk, b, c). Davis and Harris (2020) also examined five small retailers to explore internal control strategies used to prevent and detect employee fraud. This study also includes different types of small businesses in the sample, as suggested by Kennedy (2018), as the differences may affect operating procedures and opportunities for fraud.

4.2 Data coding and analysis

This study uses document analysis to examine court documents. Document analysis is an analysis of documents in order to gather facts (Owen, 2014). Prior (2003, p. 26) contends that documents should be considered as situated products rather than as fixed or stable objects in the world; they are produced in social settings and should always be regarded as collective (social) products. A multiple case study using court cases provides new insights by "bringing to life" the realities of fraud and the law that frames it through the multiple accounts from fraudsters, victims, and the community caught up in legal actions. The court case narratives provide a glimpse of how the impact of employee fraud is experienced by the victims, an aspect that is often neglected in the literature. Unlike previous studies, the recommended prevention and deterrence strategies are driven by the analysis of these multiple court cases (e.g., Stone, 2016; Jackson et al., 2010).

Each court case is documented in a verdict (e.g., 4–18 pages), and this is the unit of analysis in this study. The documents occupy a very important position compared to non-court documents, such as newspaper articles or radio or television reports. However, we are mindful that "the facts [we] will find in these documents have been selected by the recorder" (see Caulley, 1983). We concur with Gottschalk's (2020) suggestion to move away from case-by-case discussion[2] and focus on relationships between concepts. For example, the age of the offender is assumed to influence the type of crime committed, but the sentence for a crime is influenced by crime category and crime motive (Gottschalk, 2020). Sensitive identifying information, such as names and positions, is replaced with pseudonyms. Some variables, such as age, were easy to find in the documents, but it was more difficult to find and classify the fraud diamond elements. As the specific elements of the fraud diamond might not necessarily be described in some paragraphs or pages of the court cases, the entire text was individually read by the researchers. The most challenging element was determining whether the rationalization was internal or external. After deliberation, the consensus was reached to resolve differences in interpretations and by referring to previous research on rationalization. Nonetheless, the interpretations were based on the information made available in the cases, and biases may be introduced, which is limited to researchers' understanding of the context, the outsiders' perspective.

[2] We want to credit one of the reviewers for this suggestion which we believe has significantly improved this study.

We used thematic analysis to search for patterns and themes in the court documents according to the fraud diamond elements: pressure, rationalization, opportunity, and capability. The analysis involved segmentation, categorization, and relinking of different concepts of interest (Grbich, 2007; Owen, 2014). We also identified other relevant concepts, such as fraud symptoms, to help gain a deeper understanding of the contextual nature of fraud offenses. All coding was independently verified by two researchers. Clarifying the leading researcher's biases and reaching consensus are common rigorous measures of reliability and validity (Creswell & Poth, 2018). This process was replicated for each of the 18 cases separately, and the results were then aggregated. The small number of cases limited our analysis; we therefore only undertook descriptive analysis.

5 Findings and discussion

5.1 Findings

We found that the nature of those businesses victimized by employee fraud was mixed, but geographically, most businesses were in the North Island of New Zealand. The victims were small businesses providing services (such as computing services) (44%), construction companies (22%), agriculture-related companies (17%), and manufacturing companies (5%)[3]. Some companies had been granted name suppression by the courts. All but two were located in the North Island of New Zealand. As shown in Table 2, the average fraud loss for the 18 cases was approximately $190,000, with the highest fraud losses recorded in just two cases. Fraud losses committed by managerial and nonmanagerial employees were higher in incidence but lower in average amount. Judge PD Rollo mentioned in Clarice's case, at [10], *"... your attempts to divert the company away from the enormity of your fraudulent actions, by your false claims on apprehension. This was a gross breach of trust by someone in a position of considerable responsibility in the company...."*.

The average length of time that fraud was undertaken in our sample spanned 25 months. In the case of Olga, the fraud was committed as soon as she started work with her first employer, but her actions were not reported to the police. She went on to commit fraud against two other employers within 18 months in the same city, possibly because her employment history had not been marred by her previous fraudulent behaviour. In Matthew's case, at [23], Judge AC Roberts remarked, *"The business was established by the principal and operated for 20 years and for a third of that time you rorted your employer. Virtually single-handedly, you almost brought that company to its knees and you cannot reinstate."* Furthermore, at [33], the judge said, *"... Employers are not there literally to be fleeced at will."*

The average age of the fraudsters was 48. At this age, fraudsters tend to be in a comfortable position with more influence in terms of seniority. As shown in Tables 2, in New Zealand younger people were also entrusted with both managerial and nonmanagerial positions. Female fraudsters outnumbered male fraudsters by 3:1 in all

[3] Untabulated.

Table 2 Perpetrator characteristics by position

		Average Age	Average fraud losses (4)	No. of cases	Average length of fraud	Gender		Sentencing			
						Male	Female	Home	Community	Reparation	Jail
Position[+] (Capability)	Both managerial and nonmanagerial	28	291,434.00	2	39 months	0 (0%)	2 (11%)	0	0	0	2
	Managerial	43	141,834.172	10	27 months	3 (16%)	7 (39%)	3	1	4	7
	Nonmanagerial	60	159,712.97	4	18 months	1 (6%)	3 (16%)	2	0	3	1
Total						4	12	5	1	7	10
Average for all cases		48	$189,227.82		25 months						

[#]In two cases, the perpetrator's position and age were not disclosed. Age was not mentioned in 7 cases

positions. In terms of the seriousness of the crime, the sentencing was numerically coded as home detention, community service, reparation, and jail sentence. As illustrated in Tables 2, ten fraudsters (55%) were jailed but some of the employee fraudsters received multiple sentences. For example, Allison, age 60, received seven and a half months of home detention and was required to pay reparation of $148,900 at not less than $300 per week. For those who received jail sentences, the sentences ranged from 20 to 54 months. On sentencing in Clarice's case, Judge PD Rollo stated, at [14], *"… Sentencing needs to be a very strong message to all people within the community that such significant fraud on employees just cannot be tolerated. There will be condign sentences imposed by the Courts where that happens. This is required to make people responsible for what they have done and to accept responsibility.… It is a denunciation of such fraudulent prolonged and significant dishonesty".*

As shown in Tables 3, vice and family circumstances were most common as compared to financial pressure, mental health, and greed. In terms of family aspect, Helen, who was in her early 60 s, reported that she had suffered from physical and sexual abuse from a young age. However, Judge J Brewer said at [23], *"… [At this age] abusive experiences were irrelevant and that [there is] a history of dishonest offending over many years, with the latest offending being a clear abuse of trust by a woman of mature age".* Interestingly, employees in higher positions indicated financial pressure, such as Patricia who needed to support her daughter. In terms of greed, Judge JE Maze refused Olga's defense based on the financial pressure of being a single parent, as she had used fraudulently obtained money to travel overseas and send her children to private schools. The judge said the main reason for the fraud was greed. Although financial distress was the initial motive, it was greed that drove the subsequent fraud. In response to an argument about her health by Helen, Judge Roderick Joyce QC said at [102], *"The Court must approach health matters cautiously so that health does not become any kind of licence to offend and thus to avoid accountability".*

As compared to external rationalization, most of the fraudsters rationalized their fraud internally (71.9%). For example, Patricia claimed that she had only been borrowing the money and intended to repay it. Tiffany was ashamed of her actions and claimed that she did not truly know why she had done it but had continued because "it was easy". Judge Roderick Joyce QC said at [42], "*... That last admission indicates to me that you [Tiffany] and financial temptation are a risky mix and the signs are of, in this aspect of personality or character, an absence of moral fibre".* Jeremy and Pamela thought they were entitled to the money. Pamela said she had worked very hard for her employer and thus was entitled to "overtime pay". Jeremy claimed that the amount taken was less than the supposed 15% shareholding promised by the previous owner, but there was no evidence to support his entitlement claim. An example of external rationalization was Helen's claim that someone else had taken the money, diverting culpability to others rather than herself.

With regards to fraud symptoms, Table 3 shows that only two fraud symptoms were found in our sample: previous conviction (66.7%) and unusual behavior (33.3%). For example, in Frances's case, although she had no prior conviction, the judge was not convinced and said that with "… *multiple offences committed over a period of a year or more, it was not really apt to describe [her] as a first-time offender*". In Matthew's

Table 3 Perpetrator pressure and rationalization, sentencing and fraud symptoms

		Pressure					Rationalization		Fraud symptoms	
		Financial	Vice	Family	Mental	Greed	Internal	External	Previous conviction	Unusual behaviour
Position (Capability)	Both managerial and nonmanagerial	3	1	2	0	1	2	1	1	0
	Managerial	3	3	3	3	1	12	3	2	0
	Nonmanagerial	0	3	2	0	0	9	5	1	2
Total		6	7	7	3	2	23	9	4	2

case, his employer found him to be very efficient and trusted him completely. He was a hardworking person who worked long hours and even refused to take time off for his paid honeymoon.

As shown in Table 4, all victims were financially affected after being swindled by their employees. Some had to incur investigation costs ranging from $30,000 to $138,729. The average financial fraud loss was more than $200,000.[4] Moreover, prior to the fraud's discovery, one of the victim companies was already in financial distress due to the recession. One of the owners of the sampled companies, Barnaby, had to inject $35,000 of his savings intended for his children's education fund to cover some losses and Patrick, had to sell his business premises, renting it instead, sell other property, use his inheritance, and borrow to repay creditors.

Five small businesses in the sample had to cease trading; thus, the fraud caused all other employees to lose their jobs. Ten business owners suffered emotional impact, two experienced health issues, two blamed themselves for the fraud, and one encountered social disintegration with family members. For instance, a business owner, James, suffered significant emotional harm and severe breakdown, saying that he found it very difficult to trust anyone again. Two of James' customers who lost deposits to the fraudster said they had difficulty coping with emotion and felt betrayed. At [51], Judge Roderick Joyce QC in CRI-2008-005-015786 remarked,

> … my reading of what each [victim] had written on this account left me with a more acute than usual sense of the inability of the justice system to offer people in the position of Flimson [pseudonym] and Derrick [pseudonym] effective consolation, so I avoid the platitudes.

We could identify only the fraudsters' positions and not their departments from the fraud cases. For example, in Sabrina's case, Judge MBT Turner commented at [6] (a), *"… You were in a position of authority and trust. You had almost complete control over the finances of this business. No doubt your employer left you to your own devices in that regard and relied upon you being an honest person".*

As shown in Table 5, both billing and accounts payable and payroll schemes recorded more than half of the reported fraud schemes (52%). Billing and accounts payable fraud was committed largely by those in managerial positions (17 cases; 65.4%) as compared to other categories. Allison, Frances, and Patricia used their online computer access to their companies' purchasing systems to order items for their personal use from vendors, resulting in losses ranging from $63,723.81 to $166,000.

In other cases, the employees abused their access by replacing the supplier's online bank account number with their own or a family member's bank account. In doing so, Bethany and Olga were able to redirect payments intended for suppliers to their own bank accounts. Bethany even used both her partner's and her son's bank account numbers to replace various suppliers' bank accounts, ultimately stealing $147,390.87 from her employer. Any alteration to master file details should be restricted to the business owner, but as an account administrator, Bethany had full access.

[4] Three businesses received name suppression and therefore are not included in this discussion.

Table 4 Victim impact statements—consequences of employee fraud

		Financial	Investigation cost ($)	Cease trading/ employment	Emotional	Health	Social disintegration with family members	Self-blame
Position	Both managerial and nonmanagerial	2	30,000	2	1			1
	Managerial	10	138,729	2	7	1		
	Nonmanagerial	4	30,000	1	2	1	1	1
Total		16^	198,729	5	10	2	1	2

^In 2 cases, the position of the offender was not disclosed

Carol, Olga, Matthew, Jeremy, and Sabrina used their online computer access to create false suppliers and then entered their personal bank accounts as payment recipients. Sabrina deliberately altered the names of suppliers online to transfer $45,000 to her own bank account. Carol was careful to ensure that the new supplier names were similar to those of existing suppliers and then fabricated supporting documents for payments. She stole $252,402.80 in 104 transactions. Tiffany banked $312,467.27 from 68 fabricated purchasing transactions using the company's software and EFT. Olga made false payments of $350,000 to creditors that ended up in her bank account.

There were 13 mentions of payroll fraud schemes and 53.8% of them were perpetrated by employees in managerial positions. It is common for managers in small businesses to be entrusted with payroll tasks. Three common payroll fraud schemes were mentioned in the court documents: alteration of the fraudsters' own wages, working hours, and hourly/pay rate in the payroll system; unauthorized additional salary payment outside the payroll run; and unauthorized overtime, commission, holiday, and sick leave pay.

In the first and second schemes, the fraudsters' own total wages and pay rates were inflated using their online computer access, typically during the payroll run. For example, Patricia created a default of 40 working hours in the payroll system and obtained $1,700 more than she should have been paid. Carol overpaid her holiday and sick leave, amounting to $8,802.20. On five occasions, Matthew inflated his own wage payment. He also issued commission payments, supposedly to a salesperson, four times during the payroll run but altered the beneficiary bank account to his own. He took $74,235.95 from his employer in six years, which meant six years of undetected payroll schemes owing to a lack of monitoring by the small business owner, who described Matthew as a "perfectionist" and trustworthy.

We also examined whether the court documents provided details of any preventive methods and narratives of how the frauds were discovered (detection methods) so that suitable strategies could be discussed and recommended. In our sample of 18 small businesses, only two prevention methods were employed. In Pamela's case, the list of payments to be made had to be approved by the business owner. The business owner blindly signed off the requests for payments to (fictitious) suppliers, which ended up costing him $203,508 over 76 fraudulent payments. In terms of unauthorized payroll, Alice denied any wrongdoing and claimed that the company's payroll system required a responsible person, independent of her, to check and sign off on all payments, including her overtime. She was not entitled to overtime payment but insisted that the payments were transparent and expressly authorized.

The frauds in the sample were discovered by audit and forensic investigations (five cases), followed by business owners (three cases), and post resignation/dismissal investigation (three cases). Four fraud cases were discovered in the absence of the employee, such as when he or she was on vacation, and when new employees took over. Only one case indicated that a third party, a bank, had contacted the employer about suspicious transactions. Two court documents did not clearly indicate how the fraud cases had come to light. Only one company had purchased insurance against fraud, but the fraud was too large, at $198,299.84, to be completely covered by the insurance policy. In Matthew's case, the auditor noticed some irregularities,

Table 5 Fraud schemes and identified strategies

		Fraud Schemes						Fraud discovery (Detection method)	Prevention methods employed
		Asset Misappropriation	Billing & Accounts Payable	Payroll	Receivable	Other	Total		
Position (Capability)	Both managerial and nonmanagerial	1	2	1		1	5	Successor and forensic investigation	Approval by employer of list of payments to be made
	Managerial	4	10	7	6	4	31	Owner; audit; post dismissal/ resignation	
	Nonmanagerial	4	1	5		4	14	Owner; audit; absence; third party	Verification by an independent person
Total		9	13	13	6	9	50		

and when the unauthorized payments were examined, they were traced to his bank accounts (Humphreys, 2011).

6 Discussion

The importance of small businesses to the New Zealand economy was described by Judge JE Maze in Olga's case, at [3], *"... those companies were providing employment to others and were deriving an income for those who had made the capital commitment to set the business up in the first place. Such commercial entities form a significant part of the commercial picture in New Zealand. They are usually very modest. They frequently provide the individuals at the heart of those businesses with a modest return on their investment and time. Their chief importance lies in the fact that they provide employment for others. What you did, struck at the security, not only of the owners of those businesses, but importantly also, at the others who derived employment and income, and security for their lives from those businesses".*

Previous studies have reported that older male employees who occupy senior positions are particularly likely to commit fraud (e.g., Goldstraw et al., 2005; Peltier-Rivest and Lanoue, 2012; Wells, 2002). In contrast to these findings, our sample showed that women committed more and larger frauds than men, consistent with the findings of Holtfreter (2005). In terms of the seriousness of the crime, the sentencing was varied and the fraudsters who incurred the most expensive fraud losses were both jailed.

The victim impact statement in each court case was analyzed to examine the consequences of the employee frauds. All victims in our sample suffered financial losses and the additional burden of investigation costs. As Judge Roderick Joyce QC remarked in Tiffany's case, at [17], *"'White collar fraud' might be a convenient generic term, [but] what one was talking about was barefaced theft and a gross breach of trust".* Consequentially, the business owners had to sacrifice their own savings and inheritance to cover some of the losses and other obligations. According to Adam et al., (2006), the financial impact of fraud on small businesses can be so devastating that even if they survive the employee fraud, they might discontinue business. Nearly one-third of the businesses consequentially ceased and caused loss of employment to other employees. The business owners experienced more devastating emotional repercussions than financial consequences (Kennedy, 2018; Yekini et al., 2018). In our sample, the victims also suffered deteriorating health and family relationships. Kennedy (2018) suggested that different businesses might experience different types of employee fraud, but in our sample, there was no clear association between the nature of the business, the type of fraud, and fraud losses.

Fraud symptoms are the red flags that often go unnoticed or, if they are noticed, not vigorously investigated (Albrecht et al., 2019). Only two fraud symptoms were found in our sample: previous conviction and unusual behaviour. Only four fraudsters had previous convictions. According to Arnold and Bonython (2016), reoffending energizes employees with a "good" feeling that drives them to repeat their behavior. In our sample, the majority of the fraudsters were first time offenders. Previous studies suggested that many acts of fraud start with small sums without an intention to com-

mit a crime (Hess & Cottrell Jr., 2016; Kranacher et al., 2011; Levi, 2008; Wells, 2002). However, in one case, the New Zealand court refused to accept a fraudster's plea of not having a previous conviction when multiple offences were committed over a period of time. In terms of unusual behaviour, Simser (2014) noted that there are some clues that an individual intends to engage in fraudulent activity, such as working long hours and refusing paid holidays. This behaviour is quite unusual as observed in two cases in our sample. Suspicious patterns can be behavioural as well as financial (see Hess & Cottrell Jr., 2016). Being hardworking is often misconstrued as being dedicated, but in this case, the fraudsters did not want their deviant activities to be discovered.

According to Albrecht et al., (2019), fraud prevention activities are the most cost-effective of all fraud countereforts, and early fraud detection is the second most cost-effective way to fight fraud. Due to the lack of resources for a robust internal control system, many entrepreneurs must decide for themselves on the right approach (Robinson et al., 2003). In our sample, only two prevention methods were employed: authorization of supplier payment list and payroll. However, the business owners signed off the requests for payments without properly checking whether the goods and services had been delivered. Such checks could have been made based on supporting documents, such as receiving reports and whether the suppliers were indeed the company's approved suppliers. In terms of unauthorized payroll, the person responsible for verification did not perform due diligence by checking the details of the payroll transactions, especially for overtime entitlements. This could have been uncovered and stopped quickly had better checks been in place (Kidd, 2012). Although preventive strategies existed, they systematically became ineffective due to the trust the employers reposed in their employees.

In terms of a detection strategy, our study suggests that audit was a valuable detection method. However, an audit is not a legal requirement for small business owners in New Zealand. In addition, it is not the responsibility of the auditor to detect fraud, and it is possible that even if an effective audit is performed, material fraud may still remain undetected. Furthermore, the cost of auditing may outweigh the benefits (Kennedy, 2018). The four-eyes principle is therefore still the key. As Judge JE Maze rightfully remarked in Olga's case at [14], *"... In reality it is the boss, the owner of the business, who has directly handed over the money to you to fund your extravagant and dishonest lifestyle".* This is a tough reminder to small business owners to be vigilant and understand that trust is not a method of fraud control.

With reference to the elements of the fraud diamond framework, of which the *first* is motive (pressure), incentives to commit fraud can be financial pressure, vices, or living beyond one's means (Albrecht et al., 2019; ACFE, 2018, 2020; Andon & Free, 2015). According to Hess and Cottrell Jr. (2016), good people often make bad choices when facing intense pressure in their life. For example, Whitney was recovering from failed property development projects and did not have enough money to pay her spiraling personal bills (Stuff, 2012a). In contrast to previous studies, our study found that vice and family circumstances were the main sources of motive (pressure). This is consistent with New Zealand research which has reported that gambling can result in criminal activity and neglect of responsibilities, including the consequences of such actions (Browne et al., 2017).

The *second* element is opportunity. Opportunity has allowed fraudsters to incur total average fraud loss at almost a quarter of a million New Zealand dollars. Of significance, the highest average was reported in cases where the fraudsters occupied both managerial and nonmanagerial positions. These employees leveraged their complete control to bypass internal control in order to get access to business resources (Kennedy, 2018; Wells, 2002). The results showed that being in a position of responsibility played a major role in an employee fraud (see Wolfe & Hermanson, 2004). Other studies have found that those who commit employee fraud are largely low-level employees (Omar et al., 2016; Kennedy 2018). The higher the position of an individual, the bigger the opportunity to commit fraud; after all, insider fraud is a crime of opportunity (Kennedy, 2018). This opportunity element also allowed for employee fraud to last more than a year (Peltier-Rivest & Lanoue, 2012). The average age of the fraudsters in our study was 48 and generally, at this age fraudsters tend to be in a comfortable position with more seniority influence. Nonetheless, our findings also showed that younger people (on average) occupied both managerial and nonmanagerial positions and thus had more opportunity to defraud while causing the lengthiest and highest losses. Younger employees tend to be more impulsive and most likely to engage in fraud (Kennedy 2017; Omar et al., 2016; Ng & Feldman, 2009; Holtfreter, 2005). Those in managerial positions perpetrated fraud longer than those in nonmanagerial positions, consistent with the findings of Kennedy (2017) and Peltier-Rivest and Lanoue (2012). The longer a fraud is undetected, the greater the losses (ACFE, 2020). As asserted by Hess and Cottrell Jr. (2016), degradation in moral standards may happen gradually and thus be unnoticeable.

As shown in this study, those in both types of position committed the longest-lasting frauds, as the combination of opportunity and capability provided them with more time to conceal their fraud. Capability is the *fourth* element of the fraud diamond framework. In all cases, the fraudsters were capable of perpetrating online billing and accounts payable fraud schemes because they were responsible for these two functions. Billing schemes are known to be extremely expensive (Albrecht et al., 2019; ACFE 2018, 2020). Further, we found that the billing and accounts payable fraud was committed largely by those in managerial positions who had access to the company's bank accounts and who were allowed to perform EFT, a combination of opportunity and capability. As CPA Australia (2008) cautioned, even people with permission may authorize EFT payments without following procedures or disburse cash for nonbusiness expenses. Our analysis indicated that there was no verification of the purchases by an independent party or by the business owner through a purchase order approval process or verification of whether the suppliers were legitimate. When suppliers complained that they had not received payments, the business owner did not check whether the purchase invoices had actually been paid and to which bank accounts the payments had been made. In fact, there was no cross-check of suppliers and staff bank accounts to ensure that they were in fact identical to prevent faulty payments.

Consistent with Stone's (2016) expectation that payroll fraud occurs more frequently in small businesses, our sample showed that nearly one-third was fraud involving payroll. Feeling undervalued and underappreciated was the common driver of payroll fraud (Jackson et al., 2010) but as explained above, vice and gambling

were common among New Zealand fraudsters. In our sample, most fraud was perpetrated by employees in managerial positions who were also responsible for payroll. It is common for managers in small businesses to be entrusted with payroll tasks. According to Albrecht et al., (2019), the most common method is the overpayment of wages, but previous studies have not discussed the specific schemes of payroll fraud. We found that the fraudsters manipulated their online computer access to alter their own salary rates in order to increase their salary without the business owners' knowledge. In one case, the fraud lasted for six years. In all cases, the ability to alter the hourly rate, wage payment or working hours indicated the capability of the fraudster in making use of their access. This type of access should be restricted to only the owner of the business.

In terms of rationalization, the *third* element of the fraud diamond framework, the fraudsters tended to rationalize their actions to justify their intentions to avoid feeling guilty or when pleading guilty or appealing for lighter sentences in court (Othman et al., 2020; Albrecht et al., 2019). In our sample, most of the fraudsters rationalized their fraud internally and this rationalization was more frequently used by those in managerial positions compared to those in nonmanagerial positions. The fraudulent leader has the ability to rationalize bad decisions that are not even ethical (Chenguel, 2020). This perceived entitlement was internalized to compensate for "injustice" (Kennedy, 2018).

Based on the analysis, preventive strategies should start before employment and continue during the course of employment. Although only four fraudsters in our sample had prior convictions, a background check that cost as little as the first day's salary—simply asking previous employers whether they would rehire the applicants—could have saved the companies an average of $139,758.62 (Gubbins, 2017, 2018; Brody et al., 2015; Shao, 2016; Laufer, 2011; Kramer, 2015). Fraud risk is heightened when people with previous fraud convictions are employed (ACFE, 2018, 2020). However, it is also possible that the large majority of fraudsters in the sample who had committed fraud in the past had been fired but not reported, and thus not prosecuted, for the fraud (see Kennedy, 2018). There was an obvious lack of monitoring and independent verification by the small business owners who had entrusted their star employees with incompatible duties. Trust is not a method of fraud control, and when it is combined with opportunity and capability, fraud is inevitable. The lengthiest fraud in our sample lasted more than six years, indicating fault in addition to fraud (Kumar et al., 2018). If fraudsters believe that they can avoid discovery, they are more likely to commit further crimes (Kranacher et al., 2011; Hess & Cottrell, Jr, 2016; Levi, 2008). Most of the fraud cases were uncovered by audits. Both the knowledge that auditors were present, and the possibility of surprise audits discouraged fraudulent behavior (Murphy & Free, 2016; Wells, 2002). However, audits can be expensive for small businesses, so they need to self-police by exercising the four-eyes principle.

In the four-eyes principle, it is critical during the course of employment for owners to look for suspicious patterns and unusual transactions periodically and continuously (Hess & Cottrell Jr., 2016). Extra vigilance should be the ultimate priority given the perceived vulnerability of small businesses to fraud compared to larger organizations. In terms of access to the company's bank account, the owner should

have sole access and manage EFT transactions to ensure that payments are not made to employees except for payroll. Before any purchase can be made, the purchase order should be approved by the owner or an independent person to verify both the items ordered and the vendors. Any payment to vendors should be accompanied by verified supporting documents. A payroll summary and vendors' statements should be reviewed regularly to identify sudden increases and unusual transactions. Any alterations of vendors, bank accounts, wage payments, hourly rates and working hours should be made only by the owner (Albrecht et al., 2019; Moroney et al., 2017; Hess & Cottrell Jr., 2016). Setting authorization limits restricts employees' ability to commit misconduct and fraud (Parkes et al., 2016; Kranacher et al., 2017; Stuff, 2012b). As Kranacher et al., (2011) emphasized, there is a greater fraud risk if an employee has access privileges beyond those required to perform his or her assigned job. Passwords to access bank accounts should be routinely changed and not shared even with trusted employees.

Costless practices such as mandatory vacation periods and job rotation could be useful, as nearly half of the fraud cases in the sample were discovered when the employees were not working or no longer working for the company (Hess & Cottrell Jr., 2016; Stone, 2016). In small businesses, owners have the unique opportunity to build a more cohesive ethical culture by communicating clear messages on the ethical values expected of their employees (Hess & Cottrell Jr, 2016). According to Carland et al., (2001), the most effective and real deterrence is the fear of informal and social sanctions along with the perception that unethical actions and fraudulent behaviors are not tolerated. In this regard, business owners should set the example. Employees need to be convinced that the owners will not hesitate to report anybody responsible for fraud to the authorities, and they should be encouraged to speak up and raise concerns over any suspicious behaviour or actions (Hess & Cottrell Jr., 2016; Kranacher et al., 2011; Albrecht et al., 2019; Sow et al., 2018; Omar et al. 2016)). Nonetheless, if an employee is dishonest, even the best internal and management control systems will not be able to prevent fraud, as the likelihood of committing fraud is most directly proportional to an individual's level of personal ethics (Jackson et al., 2010; Albrecht et al., 2019; ACFE, 2008; PWC, 2018; Merchant & Van der Stede, 2007; Deschamps, 2019).

7 Conclusions

The fraud diamond theory, an expanded version of the fraud triangle, offers insightful information regarding the various factors that influence an individual's decision to commit fraud: opportunity, pressure, rationalization, and capability. For example, a person who has the opportunity, motivation, and rationalization may not be able to execute fraud in the absence of the capability element, in our case, the capability to get and manipulate online computer access to commit fraud. Framed by fraud diamond theory, this study examined 18 court documents of employee fraud between 2006 and 2020 in order to understand how and why employees used online computer access to commit fraud in New Zealand small businesses. In addition to the pressure and rationalization elements, the cases highlighted the devastating and pervasive

nature of employee fraud. In particular, when the opportunity and capability elements of the fraud diamond theory framework are combined, the employee fraud tends to be lengthier and costlier, indicating the critical importance of management control as part of internal control systems in mitigating such fraud.

The total recorded fraud losses suffered by the small businesses were close to $200,000, and this amount was doubled by the additional costs of audits and investigations. The small businesses were victimized through billing and accounts payable and payroll schemes. Most of the frauds were committed by trusted middle-aged (on average) women with no prior convictions who gained the opportunity and capability through their positions to fuel their addictions and address their family circumstances. Those who occupied both managerial and nonmanagerial positions committed the most expensive and longest frauds. There was no direct link between the nature of the business and fraud losses and length. However, the frauds caused five small businesses to cease trading and caused severe emotional harm to the business owners. Only two preventive strategies were identified, but as is apparent, they had not been sufficiently implemented to prevent the frauds. All four fraud diamond theory elements provided insight into the contextual nature of such fraud and a better understanding of why and how employees committed fraud in small businesses in New Zealand.

In contrast to public companies, there has been limited research on small businesses due to the seemingly insignificant size of the stakeholders involved. However, research in this area should be pursued, as the devastating nature of employee fraud can be disastrous to the communities and economies immediately surrounding a business. The findings of this study are limited to the cases made available in the database; thus, we cannot claim generalizability to other employee fraud cases in New Zealand. In addition, it is possible that many other frauds were undetected, and fraudsters were not reported nor prosecuted. Future research might benefit from more cases being added to the database to allow for interindustry comparison and longitudinal analysis. We focused on the locality of the New Zealand jurisdiction, which determines the prosecution of the crimes and the associated sentencing but lacks generalizability; similar cases may have been investigated and prosecuted differently in other countries on the basis of national and institutional shared values and cultures.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions

References

Albrecht, C., Kranacher, M. J., & Albrecht, W. S. (2008). Asset misappropriation research white paper for the Institute of Fraud Prevention, 1–22. Retrieved June 20, 2020 from www.theifp.org/research-grants/IFP-Whitepaper-5.pdf

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2019). *Fraud Examination* (6th Edition). Cengage Learning: Boston

Alstete, J. (2006). Inside advice on educating managers for preventing employee theft". *International Journal of Retail & Distribution Management*, 34(11), 833–844. https://doi.org/10.1108/09590550610710237

Altman, E. (1968). Financial ratios. Discriminant analysis and the prediction of corporate Bankruptcy. *The Journal of Finance*, 23(4), 589–609

Andon, P., & Free, C. (2015). Pathways to accountant fraud: Australian evidence and analysis. *Accounting Research Journal*, 28(1), 10–44

Association of Certified Fraud Examiners (2018). Report to the nations on occupational fraud and abuse. Retrieved June 20, 2020 from https://www.acfe.com/report-to-the-nations/2018/

Association of Certified Fraud Examiners. (2020). Report to the nations on occupational fraud and abuse. Retrieved June 20, 2020, from https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Arnold, B. B., & Bonython, B. (2016). Villains, victims and bystanders in financial crime. In M. Dion, D. Weisstub, & J. Richet (Eds.), *Financial Crimes: Psychological, Technological, and Ethical Issues* (pp. 167–198). Springer: AG. doi: https://doi.org/10.1007/978-3-319-32419-7_8

Aztech Engineering (n.d). About. Retrieved July 27 (2020). from https://www.aztechengineering.co.nz/about (Accessed 27 July 2020)

Beneish, M. (1999). The detection of earnings manipulation. *Financial Analyst Journal*, 55, 24–36

Benford, F. (1938). The Law of Anomalous Numbers. *Proceedings of the American Philosophical Society*, 78, 551–572

Brody, R. G., Perri, F. S., & Van Buren, H. J. (2015). Further beyond the basic background check: Predicting future unethical behaviour. *Business and Society Review*, 120(4), 549–576. Doi: https://doi.org/10.1111/basr.12074

Browne, M., Bellringer, M., Greer, N., Kolandai-Matchett, K., Rawat, V., Langham, E. … Abbott, K. P. (2017). M. Measuring the Burden of Gambling Harm in New Zealand, Retrieved October 12, 2021 from https://www.health.govt.nz/system/files/documents/publications/measuring_the_burden_of_gambling_harm_in_new_zealand.pdf

Bunn, E., Ethridge, J., & Crow, K. (2019). Fraud in small businesses: A Preliminary Study. *Journal of Accounting and Finance*, 19(3), 24–32. doi: https://doi.org/10.33423/jaf.v19i3.2030

Chenguel, M. B. (2020). *Financial Fraud and Managers, Causes and Effects.* Retrieved October 12, 2021 from DOI: https://doi.org/10.5772/intechopen.93494

Committee of Sponsoring Organizations (COSO). (2013). The 2013 COSO framework & SOX compliance. Retrieved July 7, 2020 from https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf

Cant, M. C., Wiid, J. A., & Kallier, S. M. (2013). Small business owners' perceptions of moral behaviour and employee theft in the small business sector of Nigeria. *Gender and Behaviour*, 11(2), 5775–5787

Carland, J. W., Carland, J. C., & Carland, J. W. (2001). Fraud: A concomitant cause of small business failure. *The Entrepreneurial Executive*, 6, 73–108

Caulley, D. N. (1983). Document analysis in program evaluation. *Evaluation and Program Planning: An International Journal*, 6, 19–29

Corns, M. C. (1971). *How to audit a bank. Boston*. M.A. Bankers Publishing company

CPA Australia (2008). Internal controls for small business. Retrieved July 27, 2020 from https://www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/business/internal-controls-for-small-business.pdf?la=en (Accessed 27 July 2020)

Cressey, D. (1953). *Other People's Money: A Study in the social psychology of embezzlement*. Glencoe: The Free Press

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design Choosing among Five Approaches*. 4th Edition, Thousand Oaks, California

Davis, M. V. (2019). Strategies to Prevent and Detect Occupational Fraud in Small Retail Businesses", *Walden Dissertations and Doctoral Studies*, 6887. Retrieved June 20, 2020, from https://scholarworks.waldenu.edu/dissertations/6887

Davis, M. V., & Haris, I. I. I., D (2020). Strategies to Prevent and Detect Occupational Fraud in Small Retail Businesses. *International Journal of Applied Management and Technology*, 19(4), 40–61

Deschamps, C. (2019). Stages of management control in a large public organization: from top to frontline managers. *Journal of Management Control*, 30, 153–184. https://doi.org/10.1007/s00187-019-00282-z

Digital Inclusion Research Group. (2017). Digital new zealanders: The pulse of our nation. A Report to MBIE and DIA. July 27, 2020 from https://www.mbie.govt.nz/dmsdocument/3228-digital-new-zealanders-the-pulse-of-our-nation-pdf

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555–579

Feng, N. C. (2018). The impact of noncompliance and internal control deficiencies on going concern audit opinions and viability of nonprofit charitable organizations. *Journal of Accounting, Auditing & Finance*, 35(3), 637–663. doi: https://doi.org/10.1177/0148558X18774904

Free, C. (2015). Looking through the fraud triangle: a review and call for new directions". *Meditari Accountancy Research*, 23(2), 175–196. https://doi.org/10.1108/MEDAR-02-2015-0009

Free, C., & Murphy, P. (2015). The ties that bind: the decision to co-offend in fraud". *Contemporary Accounting Research*, 32(1), 18–54

Gillam, M. (2018). Exclusive: Business Pays $4000 For Investigator After Cops Refuse. Retrieved August 8, 2020 from https://www.theinvestigators.co.nz/news/business-pays-4000-for-investigator-after-cops-refuse/

Goldstraw, J., Smith, R. G., & Sakurai, Y. (2005). Gender and serious fraud in Australia and New Zealand. *Trends & Issues in crime and criminal justice*, 292, 1–6. Retrieved June 24, 2020 from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.560.5887&rep=rep1&type=pdf

Gottschalk, P. (2020). Coding and analysing police crime court cases. *The Police Journal*, 83, 339–363. doi:https://doi.org/10.1350/pojo.2010.83.4.502

Gottschalk, P. (2020b). Convenience in White-Collar Crime: A Case Study of Corruption among Friends in Norway, *Criminal Justice Studies.* Retrieved June 24, 2020 from https://doi.org/10.1080/1478601X.2020.1723084

Gottschalk, P. (2020c). Convenience in White-Collar Crime: A Case Study of Unknown Perpetrator at Popcorn Time. *Deviant Behaviour*, Retrieved June 24, 2020 from https://doi.org/10.1080/01639625.2020.1771129

Grbich, C. (2007). *Qualitative data analysis: An Introduction*. London, UK: Thousand Oaks, CA: SAGE Publications

Gubbins, C. (2018). Screen test – casuals too.Employment Today, May, 33–35

Gubbins, C. (2017). Screen check – How to avoid hiring mistakes",Employment Today, May 28–30

Haugen, S., & Roger Selin, J. (1999). Identifying and controlling computer crime and employee fraud". *Industrial Management & Data Systems*, 99(8), 340–344. https://doi.org/10.1108/02635579910262544

Hay, D. (2015). The frontiers of auditing research. *Meditari Accountancy Research*, 23(2), 158–174. https://doi.org/10.1108/MEDAR-12-2014-0062

Hess, M. F., & Cottrell, J. H. Jr. (2016). Fraud risk management: A small business perspective. *Business Horizon*, 59(1), 13–18

Hight, J. J. (2015). Limiting Leukophobia: Looking Beyond Lockup. Debunking the Strategy of Turning White Collars Orange. Retrieved July 7, 2020 from https://works.bepress.com/jared_hight/1/

Homer, E. M. (2020). Testing the fraud triangle: a systematic review. *Journal of Financial Crime*, 27(1), 172–187. Doi: https://doi.org/10.1108/JFC-12-2018-0136

Holtfreter, K. (2005). Is occupational fraud "typical" white collar crime? A comparison of individual and organizational characteristics. *Journal of Criminal Justice*, 33, 353–365

Huber, W. D. (2017). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research*, 12(2), 28–49

Humphreys, L. (2011). Auto city manager stole from company. Retrieved July 2, 2020 from http://www.stuff.co.nz/national/crime/5746268/Auto-City-manager-stole-from-company

Jackson, K. R., Holland, D. V., Albrecht, C., & Woolstenhulme, D. R. (2010). Fraud isn't just for big business: Understanding the drivers, consequences, and prevention of fraud in small business. *The Journal of International Management Studies*, 5(1), 160–164

Johnson, G., & Rudesill, C. (2001). An investigation into fraud prevention and detection of small businesses in the United States: responsibilities of auditors, managers, and business owners. *Accounting Forum*, 25(1), 56–78

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: crime scripts, business characteristics, efforts, and benefits. *Crime Science*, 9(13), https://doi.org/10.1186/s40163-020-00119-4

Kennedy, J. P. (2018). Asset misappropriation in small businesses. *Journal of Financial Crime*, 25(2), 369–383. Doi: https://doi.org/10.1108/JFC-01-2017-004

Kennedy, J. (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

Kidd, R. (2012). Home detention for 81 dishonesty counts. Retrieved July 7, 2020 from http://www.stuff.co.nz/waikato-times/news/6286553/Home-detention-for-81-dishonesty-counts

Kirkwood, J., & Viitanen, T. (2015). What is challenging New Zealander Business Owners?. *University of Otago Business School.* Retrieved July 27, 2020 from http://www.business.otago.ac.nz/mgmt/staff/What'schallenging-New-Zealand-Business-owners.pdf

KPMG. (2020). Global profiles of the fraudster: Technology enables and weal controls fuel the fraud. Retrieved August 11, 2020 from https://home.kpmg/xx/en/home/insights/2016/05/global-profiles-of-the-fraudster.html

Kramer, B. (2015). Trust, but verify: fraud in small businesses. *Journal of Small Business and Enterprise Development*, 22(1), 4–20. https://doi.org/10.1108/JSBED-08-2012-0097

Kranacher, M., Riley, R. A., & Wells, J. T. (2011). *Forensic Accounting and Fraud Examination*. New Jersey: John Wiley & Sons

Kumar, K., Bhattacharya, S., & Hicks, R. (2018). Employee perceptions of organization culture with respect to fraud – where to look and what to look for. *Pacific Accounting Review*, 30(2), 187–198. https://doi.org/10.1108/PAR-05-2017-0033

Laufer, D. (2011). Small business entrepreneurs: A focus on fraud risk and prevention. *American Journal of Economics and Business Administration*, 3(2), 401–404

Levi, M. (2008). Motivations and criminal careers of long-firm fraudsters. In M. Levi (Ed.), *The Phantom Capitalists: The organization and control of long-firm fraud* (pp. 85–125). Aldershot: Ashgate

Lofland, C., & McNela, A. (2014). What's is your fraud IQ? *Journal of Accountancy*, 27(3), 46–50

Max Pennington Auto City (n.d). About AutoCity. Retrieved July 27 (2020). from https://www.autocity.co.nz/about-us/

MBIE (2015). Small businesses in New Zealand. How do they compare with larger firms? Retrieved July 5, 2020 from https://www.mbie.govt.nz/assets/30e852cf56/small-business-factsheet-2017.pdf

Merchant, K. A., & Van der Stede, W. A. (2007). *Management control systems: Performance measurement, evaluation and incentives* (2nd ed.). Upper Saddle River: Prentice Hall

Moroney, R., Campbell, F., & Hamilton, J. (2017). *Auditing A Practical Approach* (3rd edition), John Wiley & Sons Australia, Ltd., Queensland Australia

Murphy, P. R., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. *Behavioral Research in Accounting*, 28(1), 41–56

Ng, T. W., & Feldman, D. C. (2009). Re-examining the relationship between age and voluntary turnover. *Journal of Vocational Behavior*, 74(3), 283–294

Nigrini, M. J. (2019). The patterns of the numbers used in occupational fraud schemes. *Managerial Auditing Journal*, 34(5), 602–622

NZentrepreneur (2017). Kiwi small-and medium-sized businesses lucrative targets for cybercrime, ransomware. Retrieved from June 20, 2018 from https://nzentrepreneur.co.nz/kiwi-small-medium-sized-businesses-lucrative-targets-cybercrime-ransomware/

Omar, M., Nawawi, A., & Salin, A. S. A. P. (2016). The causes, impact and prevention of employee fraud – A case study of an automotive company. *Journal of Financial Crime*, 23(2), 1012–1027. Doi: https://doi.org/10.1108/JFC-04-2015-0020

Othman, R., Laswad, F., & Berkahn, M. (2020). Financial C.R.I.M.Es in Small Entities: Causes and Consequences. *Journal of Financial Crime, Advance online publication*. doi: https://doi.org/10.1108/JFC-03-2020-0032

Owen, G. T. (2014). Qualitative methods in Higher Education Policy Analysis: Using Interviews and Document Analysis. *The Qualitative Report*, 19(52), 1–19

Parkes, A., Considine, B., Oleson, K., & Blount, Y. (2016). *Accounting Information System* (5th ed.). John Wiley & Sons Australia Ltd: Queensland, Australia

Peltier-Rivest, D. (2009). An analysis of the victims of occupational fraud: a Canadian perspective. *Journal of Financial Crime*, 16(1), 60–66

Peltier-Rivest, D., & Lanoue, N. (2012). Thieves from within: occupational fraud in Canada. *Journal of Financial Crime*, 19(1), 54–64

Prior, L. (2003). *Using documents in social research*. London, UK: Thousand Oaks, CA: Sage Publications
PWC. (2018). PwC's 2018 Global Economic Crime Survey – New Zealand. Retrieved July 6, 2020 from https://www.pwc.co.nz/pdfs/2018pdfs/pwc-nz-global-economic-crime-survey-2018.pdf
Robinson, D., van der Mescht, H., & Lancaster, J. (2003). Ethics beyond the code of conduct—understanding the ethical dilemmas of entrepreneurs. *Meditari Accountancy Research*, 11(1), 113–128. https://doi.org/10.1108/10222529200300008
Ruankaew, T. (2016). Beyond the fraud diamond. *International Journal of Business Management and Economic Research*, 7(1), 474–476
Schaper, M. T., & Weber, P. (2012). Understanding small business scams. *Journal of Enterprising Culture*, 20(3), 333–356
Scoop (2020). Dawn of New Digital Era: New Zealand SMEs Embrace Tech To Futureproof Operations, Retrieved October 11, 2021 from https://www.scoop.co.nz/stories/BU2007/S00511/dawn-of-new-digital-era-new-zealand-smes-embrace-tech-to-futureproof-operations.htm
Shao, S. (2016). Best Practices for Internal Controls to Prevent Occupational Fraud in Small Businesses? *University Honors Theses*, Paper 310. Retrieved July 6, 2020 from https://pdxscholar.library.pdx.edu/honorstheses/310
Simser, J. (2014). Culpable insiders-the enemy within, the victim without. *Journal of Financial Crime*, 21, 310–320. Doi: https://doi.org/10.1108/JFC-11-2013-0068
Smith, S., Hrncir, T., & Metts, S. (2013). Small business fraud and the trusted employee. Retrieved July 11, 2020 from https://www.acfe.com/article.aspx?id=4294976289
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 and Research*, 22, 39–62
Stone, R. (2016). Fraud, security, and controls in small businesses: A proposed research agenda. *Journal of Business*, 1(3), 15–21
Stuff (2012a). Fraudster files for bankruptcy. Retrieved August 12, 2020 from http://www.stuff.co.nz/waikato-times/7062717/Fraudster-files-for-bankruptcy
Stuff (2012b). Worker uses false bills to get $44,000. Retrieved July 6, 2020 from http://www.stuff.co.nz/southland-times/news/court/6978195/Worker-uses-false-bills-to-get-44-000
Sow, A. N., Basiruddin, R., Mohammad, J., & Abdul-Rasid, S. Z. (2018). Fraud prevention in Malaysian small and medium enterprises (SMEs). *Journal of Financial Crime*, 25(2), 499–517. doi: https://doi.org/10.1108/JFC-05-2017-0049
Wells, J. T. (2002). Occupational fraud: the audit as deterrent.*Journal of Accountancy*, April 24–28
Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal*, 74(12), 38–42
Yekini, K., Ohalehi, P., Oguchi, I., & Abiola, J. (2018). Workplace fraud and theft in SMEs – Evidence from the mobile telephone sector in Nigeria. *Journal of Financial Crime*, 25(4), 969–983. Doi: https://doi.org/10.1108/JFC-03-2017-0025
Yogi-Prabowo, H. (2014). To be corrupt or not to be corrupt: Understanding the behavioral side of corruption in Indonesia. *Journal of Money Laundering and Control*, 17, 306–326
Zarzycka, E., Dobroszek, J., Lepistö, L., & Moilanen, S. (2019). Coexistence of innovation and standardization: Evidence from the lean environment of business process outsourcing. *Journal of Management Control*, 30, 251–286 (2019). https://doi.org/10.1007/s00187-019-00284-x