2020

Strategies to Mitigate the Effects of Identity Theft in the Hospitality Industry

Patricia Lee Jirsa
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Patricia L. Jirsa

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Ronald Jones, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Kevin Davies, Committee Member, Doctor of Business Administration Faculty

Dr. Alexandre Lazo, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Strategies to Mitigate the Effects of Identity Theft in the Hospitality Industry

by

Patricia L. Jirsa

MBA, Utica College, 2008

BS, Carroll College, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2020

Abstract

Leaders in the U.S. hospitality industry experience significant losses in profitability, increased mitigation cost, and reduced revenues because of business and consumer identity theft. Grounded in the fraud triangle theory and the fraud diamond theory, the purpose of this qualitative multiple-case study was to explore strategies leaders in the hospitality industry use to mitigate identity theft. A purposeful sample of 5 leaders of 5 different hospitality businesses in Montana participated in the study. Data were collected through semistructured interviews, member checking, and a review of company documents. During data analysis using Yin's 5-step process, 3 key themes emerged: a new technology strategy, a training and educating strategy, and a vigilance strategy. The findings indicated that leaders in the hospitality industry mitigate the effects of identity theft by implementing strategies to use up-to-date technology, train employees, educate consumers, and improve their vigilance. The implications for positive social change include the potential for leaders in the U.S. hospitality industry to increase consumer confidence, improve security for consumer data, and reduce consumers' financial losses. Further social change implications include increasing revenues for businesses, decreasing costs to customers, and fostering new job opportunities, all contributing to a healthy, robust growing economy.

Strategies to Mitigate the Effects of Identity Theft in the Hospitality Industry

by

Patricia L. Jirsa

MBA, Utica College, 2008

BS, Carroll College, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2020

Dedication

I dedicate this study to the memory of my father, Clifford Madsen. He made me promise long ago that I would “go all the way”. During his life he constantly challenged me to never stop learning. He was my rock and my strength. If he was still alive, I hope he would be proud at what I have accomplished.

To my husband, Edward Jirsa, I owe a debt a gratitude. He was always there for me. He constantly reminded me that I could do it, and was always there to listen to me vent, and help me over the tough spots. Without him I never would have finished this journey.

To my daughter and granddaughters, Stephanie Anderson, Liana Anderson, and Leahloni Anderson, who have been with me for this journey, I hope I have emulated the strength and persistence to meet and overcome any challenge and provided a role model for them. I am very grateful for their support and understanding when I was not able to be there for various family functions and was always at the computer working.

Finally, I dedicate this study to my two Australian Shepherd dogs, Blaze and Storm. They were by my side for the entire journey until they both passed away. They were my rock and always knew when I needed a hug. This study is as much theirs as it is mine.

I did not go through this journey alone. The sacrifices made by my family and their undying support and understanding were critical to my success. We all did it together, and for that I am forever grateful.

Acknowledgments

When I obtained my Associate's and my Bachelor's degrees, I thought I was done. However, my desire to keep learning led me to obtain my Master's degree. I would have stopped there but for the encouragement of my family, friends, and co-workers who knew I had it in me to go further. Their support and encouragement was instrumental in starting the journey and sticking with it to the end.

I acknowledge the support and guidance of my chair, Dr. Ronald Jones. Part way through this journey I had decided to give up. Then Dr. Ronald Jones became my chair. He understood what I was feeling and provided the needed guidance and support to help me make it to the end. It was a long journey, but he was there to the end. I will be forever grateful for all he has done for me. Without his help and support, I would not have stuck with it. I thank Dr. Jorge Gayton, Dr. Julie Bonner, and Dr. Kevin Davies who all served me well as second committee members. I thank Dr. Alexandre Lazo who served as my university research reviewer.

I would be remiss if I did not mention the staff at Walden University as well. Everyone I spoke with and worked with were very supportive and understanding. They constantly reminded me that I can do this and that they are there to help along the way. I was never alone on this journey. I thank you all for everything you did to help me get to the successful end of this journey. May God richly bless each one of you.

Table of Contents

List of Tables

Section 1: Foundation of the Study

According to information included in the Consumer Sentinel Network Data Book published by the U.S. Federal Trade Commission (Federal Trade Commission, 2018), one in five people are victims of identity theft or imposter scams totaling $328 million in losses to the victims in 2017. The top three identity thefts reported were credit card fraud, employment or tax-related fraud, and phone or utilities fraud (Federal Trade Commission, 2018). Identity theft and related frauds affect everyone including consumers, financial institutions, large and small businesses, and government agencies (Thorne & Stryker, 2018). Leaders in the hospitality industry can mitigate the financial losses resulting from identity theft through the implementation of effective strategies and internal controls (Roden, Cox, & Joung-Yeon, 2016).

Background of the Problem

The hospitality industry includes hotels, restaurants, casinos, bars, theme parks, and movie theaters (Global Hospitality Portal, 2018). The hospitality industry loses 5% of total revenues annually to identity theft (ACFE Report to the Nation, 2018; Sow, Basiruddin, Mohammad, & Rasid, 2018). Data breaches might remain undetected for months or years, resulting in significant financial losses to businesses in the hospitality industry (Bjorke & May, 2016). Organizations that were victims of fraud, which include consumer and commercial identity theft and imposter scams, sustained twice the amount of losses as those organizations with antifraud controls in place (ACFE Report to the Nation, 2018). Total fraud losses for 2017 were $905 million, with a total of $328 million from identity theft and imposter scams (Federal Trade Commission, 2018). The statistics

presented in Price Waterhouse Cooper's 2014 Global Economic Crime Survey indicated 78% of the hospitality industry participants experienced asset misappropriation, with the primary external fraud to be credit card and identity fraud. Leaders pass these losses in revenue to consumers through higher costs for products and services (U.S. Department of Justice, 2016).

In a study of security breaches and the resulting harm to businesses, Chong, Hutton, Richardson, and Rinaldo (2017) suggested the need for further research regarding the effect of identity theft within the hospitality industry. Iwejor (2017) acknowledged the need for additional research into internal control systems, including integrating technological applications used to reduce identity theft. Iwejor also noted that many managers do not implement the needed safeguards and internal controls because of a lack of knowledge or financial restrictions. Garcia (2018) recommended additional research into strategies that leaders in the hospitality industry need to implement to reduce instances of identity theft and fraud. A defined need existed to explore the strategies leaders in the hospitality industry use to mitigate instances of identity theft.

Problem Statement

Identity theft is one of the fastest growing crimes in the 21st century resulting in leaders in the hospitality industry experiencing reduced sales and profitability (Chong et al., 2017; Golladay, 2017). Leaders in the hospitality industry experience a loss of 0.4% - 5% of annual revenues because of identity theft, with total annual losses averaging $125 million from 2005-2014 for the U.S. hospitality industry (Romanosky, 2016). The general business problem was that identity theft negatively affects the profitability of

businesses in the hospitality industry. The specific business problem was that some leaders in the hospitality industry lack strategies to mitigate the effects of identity theft.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies leaders use in the hospitality industry to mitigate the effects of identity theft. The target population consisted of at least five leaders of five businesses in the hospitality industry, located in Montana, with successful experience in using strategies to mitigate the effects of identity theft. The implications for positive social change include increased consumer confidence, improved security for consumer data, and reduced consumer financial losses as a result of identity theft. Society benefits when leaders detect consumer identity theft prior to engaging in a business transaction with a fraudulent customer (U.S. Department of Justice, 2016).

Nature of the Study

The three research methods available are qualitative, quantitative, and mixed method (Yin, 2018). Qualitative research is an inductive approach used by researchers to collect data using open-ended questions and open discourse with participants to gain a deeper understanding of a phenomenon (Gog, 2015). I selected the qualitative research method for this study to gain a deeper understanding of a phenomenon using open-ended questions and open dialog with participants. In contrast, quantitative research is a deductive approach in which researchers use closed-ended questions and statistics to test hypotheses about the relationships or differences among variables (Gog, 2015). Researchers may also use a mixed-method approach, utilizing both quantitative and

qualitative methodologies (Yin, 2018). I did not test hypotheses among variables, which is part of a quantitative study or the quantitative portion of a mixed methods study; therefore, a quantitative or mixed method approach was not appropriate.

The three qualitative research design methods considered were: (a) ethnography, (b) phenomenology, and (c) case study. Researchers using an ethnographic design explore the cultural behaviors of participants (Small, Maher, & Kerr, 2014). I was not exploring the cultural behaviors of participants; therefore, ethnography was not an appropriate design. Phenomenological researchers focus on the shared and lived experiences of participants (Adams & van Manen, 2017). A phenomenological design was not suitable for this study because I did not collect data based on the lived experiences of participants. A case study is appropriate when the purpose of the researcher is to capture the circumstances and conditions of a real-world situation in a bounded setting (Yin, 2018). The case study design was most appropriate for this research study because I explored the real-world problem of the effect of identity theft within the bounded contextual setting of businesses in the hospitality industry.

Research Question

What strategies do some leaders in the hospitality industry use to mitigate the effects of identity theft?

Interview Questions

1. What strategies did you use to mitigate the effects of identity theft?

2. What strategies did you find to be most effective in mitigating the effects of identity theft for your business?

3. How did you assess the effectiveness of the strategies you implemented to mitigate identity theft?

4. What, if any, changes to your past process and procedures occurred to allow you to implement effective strategies to mitigate the effects of identity theft?

5. What barriers did you experience in implementing strategies to mitigate the effects of identity theft?

6. How did you overcome the barriers in implementing strategies to mitigate the effects of identity theft?

7. What other information would you like to add about the strategies used to mitigate identity theft in your business?

Conceptual Framework

The conceptual framework used in this study was a combination of the fraud triangle theory by Cressey (1953) and the fraud diamond theory by Wolfe and Hermanson (2004), who built upon the fraud triangle theory. The three key elements of the fraud triangle theory are (a) perceived pressure, which occurs when the perpetrator experiences a nonshareable problem, such as a financial problem; (b) perceived opportunity, which exists when the perpetrator believes there is a low risk of being caught; and (c) rationalization, which is when the perpetrator believes there is complete justification for the actions because of the perceived special or unusual circumstances (Mui & Mailley, 2015). The perpetrator-centric approach is the basis of the fraud triangle theory with the strength of each element used to determine the severity of the fraud (Mui & Mailley, 2015; Ruankaew, 2016).

The fraud diamond theory evolved from the research of Wolfe and Hermanson (2004), who expanded Cressey's (1953) fraud triangle theory by adding the additional element of capacity. Capacity refers to the skills and ability of the perpetrator to commit the fraud (Ruankaew, 2016). Based on the fraud diamond theory, opportunity as perceived by the perpetrator opens the door to fraud. Incentive, or pressure, along with rationalization draws the perpetrator to fraud, but capacity, or the skills and ability to commit the fraud, results in the perpetrator recognizing and taking advantage of an opportunity to commit identity theft (Ruankaew, 2016). For this study, the fraud triangle and the fraud diamond theories provided a lens for exploring the strategies leaders in the hospitality industry used to mitigate the effects of identity theft because leaders must recognize the perpetrator's rationale in order to implement effective strategies to mitigate the issue.

Operational Definitions

Business or commercial identity theft: The unauthorized entity or person using a business' identifying information for their own purposes (Cohn, 2015).

Data breaches: Unauthorized access to sensitive, protected, or confidential information resulting in the compromise or potential compromise of that data (Sen & Borle, 2015).

Identity theft: The knowing transfer or usage of another's name or identifying information with the intent to commit or to aid or abet the commission of a crime (Kahn & Linares-Zegarra, 2016).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are the preliminary expectations or presumptions that the researcher believes to be true, yet lacks the means to verify (Garcia, 2018; Yin, 2018). The first assumption was that leaders in the hospitality industry in Montana provided honest, forthright, and complete answers to the interview questions. I gained access to relevant company documents to engage in methodological triangulation. I assumed the documents were accurate, complete, and up to date.

Limitations

Limitations in a qualitative case study are the uncontrollable shortcomings or potential weaknesses that might affect the results of the study (Horga, Kaur, & Peterson, 2014; Marshall & Rossman, 2016). My reliance on semistructured interviews and a review of company documents as the data collection techniques for this study was a limitation. Another limitation was the use of the qualitative multiple case study design, which does not result in findings generalizable to a larger population. Other weaknesses in this study associated with the case study design were the potential for researcher bias to affect the credibility of the findings and researcher errors in interpretation of the interview data. I engaged the participants in member checking to mitigate any researcher biases and ensure the accuracy of my interpretation of their interview responses. The limited scope of this study might result in restricted transferability of the findings because the experience of leaders in the hospitality industry in Montana may be quite different from those leaders in the hospitality industry in a more populous state.

Delimitations

Delimitations are the beginning and ending points of a case and are the boundaries of the research study (Yin, 2018). The first delimitation for this study was the geographic region of Montana. The sample size of five leaders in the hospitality business in the state of Montana was a delimitation. Another delimitation was that I focused on strategies leaders used to mitigate the effects of identity theft and did not address other issues that may affect other leaders in the hospitality industry. The use of a combination of the fraud triangle theory and the fraud diamond theory as the conceptual framework was a delimitation.

Significance of the Study

Mitigating the effects of identity theft might result in benefits for leaders and consumers through reduced cost, safer transactions, and improved services (Chong et al., 2017; Raghaven, Desai, & Rajkumar, 2017). The findings of this study are of potential value to leaders in the hospitality industry because of gaining additional insights into effective strategies used to detect and mitigate the effects of identity theft on their businesses. The significance of this study consists of contributions to business practices and implications for positive social change.

Contribution to Business Practice

Data breaches cost businesses and consumers $51 billion in 2014 (Harrell, 2015). Although investments by leaders in modern information technology infrastructures to protect sensitive and confidential data are essential, leaders need additional educational and proactive business strategies to mitigate the effects of identity theft to their

businesses (Ranjan et al., 2012). The use of and reliance on technology in business provides convenience, but also opens businesses up to ongoing security threats (Mellado & Rosado, 2012). Leaders in the hospitality industry might implement the recommendations of this study to improve business practices through reducing the effects of identity theft. The contributions to business practices in the hospitality industry include providing leaders with effective strategies to detect identify theft, mitigate the costs associated with fraudulent transactions, increase sales because of providing adequate security measures, and improve profitability.

Implications for Social Change

Society benefits when leaders detect consumer identity theft prior to engaging in a business transaction with a fraudulent customer (U.S. Department of Justice, 2016). Leaders in the hospitality industry might adopt the recommendations of this study to mitigate the effects of identity theft for consumers. The implications for social change include improved security for consumer data, increased consumer confidence, and reduced cost to businesses in the hospitality industry that might pass on to consumers. Leaders who detect identity theft prior to consummating a fraudulent transaction provide a benefit to the affected individual who experienced theft of his or her identity.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore the strategies leaders in the hospitality industry use to reduce instances of identity theft. In this literature review, I discuss the definitions of identity theft and commercial identity theft as well as the existing fraud theories. These theories include the fraud triangle and the

fraud diamond. I reviewed the literature to compare and contrast both theories with the existing statistics available to develop strategies that may be useful to leaders in reducing instances of identity theft in the hospitality industry.

Organization of the Review

This literature review begins with defining identity theft and showing how identity theft has affected businesses through providing background details and providing the foundation for this study. The fraud theories and the literature both in favor of and against each theory will follow. This discussion includes how these theories relate to the available statistics on identity theft. The literature review concludes with a discussion of the strategies used to detect and mitigate identity theft, providing the base from which to expand and build additional strategies to aid leaders in the hospitality industry in mitigating the effects of identity theft. Information contained in literature covering the existing practices in use to detect and reduce identity theft and cyber breaches is the base from which I propose to expand by exploring the strategies leaders in the hospitality industry use to mitigate the effects of identity theft.

This literature review consists of information obtained from peer-reviewed academic journals, dissertations, scholarly seminal books, professional trade journals and reports, and journal articles specific to the hopitality industry to present the viewpoints of other researchers and as a foundation to build upon. Using the Walden University Library, the principal research databases searched included ProQuest, EBSCO Primary, Emerald Management Journals, Elseiver, Google Scholar, various departments of the United States government, Sage Premier, Business Source Complete, the Association of

Certified Fraud Examiners, CrossRef Services, and Ulrich's Periodicals Directory. Various statistical databases and reports were also researched. The search terms were *identity theft, white-collar crime, individual identity theft, cybercrimes, fraud in the hospitality industry*, *commercial identity theft, synthetic identity theft, the fraud triangle,* and the *fraud diamond*.. The sources used in this study are (a) 152 peer-reviewed scholarly journal articles, (b) nine government reports, (c) four dissertations, and (d) 12 seminal books. Of the 177 sources used, 85.8% were peer-reviewed scholarly journal articles and 115 had publication dates 2016-2020, 37 had a 2015 publication date, and 25 had publication dates from 1953-2014. A total of 81 peer-reviewed articles are unique to the literature review.

Background

Fraud is the tendency and propensity to do wrong by a person or group who intentionally uses deception and dishonest actions to obtain illegal advantage over an entity or another person regardless of the harm that the fraud may cause (Abdullahi & Mansor, 2018). Identity theft is the intentional and knowing possession or usage of an individual's or business' personal identifying information with the intent of committing or aiding the commission of a crime (Kahn & Linares-Zegarra, 2016). Identity theft is a form of fraud originally consisting of passport forgery or fake driver's licenses (DiSanto, 2015). With the advent of the internet and ecommerce, perpetrators are now able to obtain the identifying information for individuals and businesses to commit identity theft more easily (DiSanto, 2015).

Identity theft includes data breaches. Data breaches cost businesses and consumers $51 billion in 2014 (Harrell, 2015) with 43% of companies reporting a major data breach in 2013 (Chong et al., 2017). The hospitality industry experiences losses of 0.4% - 5% of annual revenues because of identity theft, equating to total annual losses averaging $125 million from 2005-2014 for the U.S. hospitality industry (Romanosky, 2016). A data breach is when personally identifiable information such as name, social security or federal identification numbers, and personal or corporate credit card or bank account information is compromised (Bjorke & May, 2016; Chong et al., 2017; Romanosky, 2016; Sen & Borle, 2015). Due to the advent of the Internet and the ease of transacting business online, millions of Americans and businesses transact business online which requires the release of personally identifiable information (Ashenmacher, 2016; DiSanto, 2015). To transact business in the 21st century society, whether in person or online, the buyer must provide personal information (Ashenmacher, 2016). The result of buyers providing personal information is that perpetrators can use the personal data to commit identity theft (Ashenmacher, 2016).

Damages from cybercrimes, including data breaches, are extremely high, with the global economy suffering financial damages in the hundreds of billions annually (Antonescu & Birau, 2015). Data breaches affect the hospitality industry through the loss of revenues, loss of trust in the brand, increased cost to customers, and loss of loyalty to the business by consumers (Chong et al., 2017). In addition to these costs are several hidden costs that leaders in the hospitality industry experience (Amato, 2016). After the breach, the annual premium for cybersecurity insurance can increase by up to 200% with

the insurance policy possibly cancelled or not renewed by the insurance company (Amato, 2016). A business owner who does not already have cybersecurity insurance in place may not be able to purchase coverage after a data breach (Amato, 2016). Data breaches could result in a downgrade of the business's credit rating, which could lead to increased interest rates on existing or new loans, and possibly compromising the business' ability to obtain new funding at a future date (Amato, 2016). The business must pay the cost of investigating the fraud to determine what happened and to quantify the direct and indirect expenses of the fraud (Romanosky, 2016). The business might also be facing the additional expense of fines, judgments, or settlements, legal expenses and remediation costs directly stemming from the breach of information (Bjorke & May, 2016). Affected customers might file a lawsuit against the business and its employees, and the credit card companies might also file suit for damages (Bjorke & May, 2016). In addition, shareholders, directors, and officers may file suit, claiming negligence, breach of fiduciary duty, breach of express or implied contract, and invasion of privacy (Bjorke & May, 2016). Business owners and leaders experience higher costs and a potential loss of customers because of data breaches. According to a study conducted by the accounting firm Deloitte & Touche LLP, the customer attrition rate after a cyber breach increases by 30%, severely impacting the revenue stream (Amato, 2016). Data breaches result in a loss of trust by customers and have a negative effect on the business' reputation, affecting any open and pending contracts (Amato, 2016). The effects of a cyberbreach can be devastating and far reaching to a business, with failure of the business the result for many owners (Bjorke & May, 2016).

With the advent of the Internet and the accessibility of computers, identity theft fraud is one of the fastest growing crimes and is the defining crime of the information age affecting individuals, businesses and governments (Golladay, 2017; Hille, Walsh, & Cleveland, 2015; Kahn & Linares-Zegarra, 2016; Zaeem, Manoharan, Yang, & Barber, 2017). Although news media publishes accounts of the larger cyber breaches, such as experienced by Target and Home Depot, smaller breaches occur with increasing regularity, but remain unpublished by the businesses affected (Ashenmacher, 2016). Fraud can cause frustration to the business and customers involved and damage the reputation and integrity of the business (Abdullahi & Mansor, 2018). The crime of identity theft occurs every 2 seconds (Loker, 2018). No organization is immune to the challenge of dealing with fraud (Azam, 2018). According to Consumer Sentinel Network Data Book, the number of fraud and identity theft reports increased from 325,519 in 2001 to 2,675,611 in 2017 (Federal Trade Commission, 2018). The most common types of identity theft involve credit cards at 42% and banking information at 38% (Harrell, 2015). Identity theft, imposter scams, and credit card fraud comprise 28.57% of all frauds reported, with total fraud losses at $905 million according to the Federal Trade Commission (2018). In 2018, 16.7 million Americans had their identity stolen (ITRC Annual Report, 2018). Business identity theft occurs when an unauthorized entity or person creates or uses the legitimate business's identifying information to steal money or product (Cohn, 2015). The exponential growth in communication technology, computers, and e-commerce contribute to the phenomenal growth in white-collar crime and identity theft (Azam, 2018). Because identity theft is fraud, the statistics for identity theft exists in

the more general fraud category, making tracking this specific white-collar crime even more difficult.

There are three types of identity theft that affect individuals and businesses alike. The more common identity theft frauds are new account theft and existing account theft (Federal Reserve Bank, 2019; Irshad & Soomro, 2018). In new account identity theft, the perpetrator obtains the identifying information of an actual person or business and opens new bank accounts or obtains new credit cards pretending to be the real person or business (Federal Reserve Bank, 2019; Irshad & Soomro, 2018). In existing account identity theft, the perpetrator uses the identifying information of an actual person or business and accesses the victim's accounts for monetary gain pretending to be the victim (Federal Reserve Bank, 2019; Irshad & Soomro, 2018). The Federal Reserve Bank (2019) termed these two types of identity fraud as *traditional identity fraud*. Because traditional identity fraudsters use the real identifying information of the victim, the financial effect to the victim is oftentimes discovered relatively quickly (Federal Reserve Bank, 2019).

The third form of identity theft is synthetic identity theft and is the most dominate form of identity theft (Irshad & Soomro, 2018; Richardson & Waldron, 2019). Synthetic identity theft occurs in three general forms: identity manipulation, identity compilation, or identity fabrication (Federal Reserve Bank, 2019). Identity manipulation is when the perpetrator creates a completely new identity using modified real identifying information of one or more victims (Federal Reserve Bank, 2019). Identity compilation is when the perpetrator uses a combination of modified real identifying information and

fictitious identifying information (Federal Reserve Bank, 2019), Identity fabrication is when the perpetrator creates completely fictitious information (Federal Reserve Bank, 2019). According the Federal Reserve Bank, synthetic identity theft is more prevalent in the United States because commerce relies heavily on social security numbers, driver's license numbers, and birth dates for verification of a persons or business' identity. The effects of synthetic identity theft can take years to uncover and usually remain undiscovered until all credit obtained under the synthetic ID is maxed out and the perpetrator stops making payments (Richardson & Waldron, 2019). The cost of the largest synthetic identity theft ring recorded to date is $200 million involving 7,000 synthetic identification cards and 25,000 credit cards (Richardson & Waldron, 2019).

The geographical location of this study was the state of Montana, with the sample population specifically from Helena. According to the Consumer Sentinel Network Data Book (Federal Trade Commission, 2018), Montana ranks 38th in the United States regarding consumer fraud, with losses totaling $1.3 million for 2017. Montana ranked 45th in the United States regarding identity theft and 36th regarding credit card fraud.

The conceptual framework for this study was a combination of Cressey's (1953) fraud triangle theory and Wolfe and Hermanson's (2004) fraud diamond theory. Wolfe and Hermanson built on the fraud triangle theory to arrive at their fraud diamond theory. A comparison of the fraud triangle and the fraud diamond by researchers indicated advantages and disadvantages of each theory exist (Mui & Mailley, 2015; Ruankaew, 2016). Strong support existed in the literature for the fraud triangle by some researchers (e.g., Free, 2015; Lokanan, 2018; Muhtar, Sutaryo, & Sriyanto, 2018), yet other

researchers preferred the fraud diamond theory (e.g., Baker, Cohanier, & Leo, 2016; Ruankaew, 2016). Some supporters of the fraud diamond theory also believed that many other factors exist that leaders must take into consideration to successfully mitigate the effects of identity theft (e.g., Baker et al., 2016; Wolfe & Hermanson, 2004). While some researchers are against the fraud triangle theory (e.g., Lokanan, 2015; McMahon, Pence, Bressler, & Bressler, 2016), others are against both the fraud triangle theory and the fraud diamond theory (e.g., Amasiatu & Shah, 2018; Eisenberg, 2017; Huber, 2017; Sen & Borle, 2015). A review of both theories and the related advantages and disadvantages of each follows below.

Fraud Triangle Theory

Businesses pass down the true expense of fraud to the consumer through increased prices for merchandise and services (Azam, 2018). According to the ACFE's 2018 Annual Report to the Nations, small businesses lose almost twice as much to fraud as larger business do. The reasoning behind this statistic is that small businesses typically have fewer resources to prevent fraud, requiring an increased level of trust in their employees due to the lack of enough robust antifraud controls (ACFE Report to the Nation, 2018). To develop appropriate strategies to mitigate the effects of identity theft, leaders must understand fraud. To attempt to better understand fraud and the criminals that perpetrate fraud, criminologist and sociologist Donald R. Cressey developed the concept of the fraud triangle in 1953 (Free, 2015; Muhtar et al., 2018; Schuchter & Levi, 2016). An understanding of the fraud triangle should be a means for leaders to develop strategies to detect and mitigate fraud (Kramer, 2015).

In 1953, Donald Cressey interviewed 200 prisoners who had been involved in embezzlement and other white-collar crime (Kramer, 2015; Mangala & Kumari, 2015). Cressey used the information obtained from the interviews in formulating the elements of the fraud triangle theory (Mangala & Kumari, 2015). The fraud triangle theory is a theoretical framework that investigators use to explain frauds committed at both individual and organizational levels (Muhtar et al., 2018; Roden et al., 2016). Three elements comprise the fraud triangle: perceived opportunity, perceived incentive or pressure, and rationalization or attitude (Free, 2015; Lokanan, 2018; Muhtar et al., 2018; Roden et al., 2016). These three elements may only exist in the mind of the perpetrator who perceives these elements to be present when planning to commit a fraud (Abdullahi & Mansor, 2018). Perceived opportunity is the circumstances that the perpetrator uses to commit the fraud, such as absent or ineffectual internal controls, or access to the identification and banking information (Free, 2015; Lokanan, 2018). If the perpetrator does not see an available opportunity, a fraud will likely not be committed (Abdullahi & Mansor, 2018). Perceived incentive or pressure is the motivation to commit the fraud, such as the need for money or desire to obtain an object or service (Free, 2015; Lokanan, 2018; Mangala & Kumari, 2015). The perpetrator must perceive a compelling reason to commit fraud, such as large personal debt, living beyond one's means, drug addiction, greed, or the desire for a better lifestyle (Abdullahi & Mansor, 2018). Perceived rationalization or attitude is how the perpetrator justifies the fraudulent action, such as a feeling of entitlement or the rush of adrenalin from the feeling of getting away with something (Free, 2015; Lokanan, 2018). An employee that feels wronged in some way

rationalizes that the money, object, or service is just, deserved compensation. By using rationalization, the perpetrator attempts to eliminate any guilt that may be present when committing the fraud. All three elements must be present for the perpetrator to commit the fraud (Abdullahi & Mansor, 2018; Cressey, 1953; Lokanan, 2018; Roden et al., 2016).

Fraud Diamond Theory

Investigators and researchers have widely used the fraud triangle to aid in understanding the reasons and motivations of perpetrators that commit fraud (Baker et al., 2016; Boyle, DeZoort, & Hermanson, 2015). However, many scholars and fraud investigators believe that Cressey's fraud triangle is inadequate and needs expanding (e.g., Huber, 2017; Lokanan, 2015; McMahon et al., 2016). In 2004, Wolfe and Hermanson introduced an expanded version of the fraud triangle called the fraud diamond (Ruankaew, 2016).

Accountants and investigators widely use the fraud triangle when investigating suspected fraudulent activities. However, many scholars and fraud investigators believe that a fourth element, capacity, provides a more comprehensive fraud model. Wolfe and Hermanson (2004) argued that even if the three elements of the fraud triangle were present, fraud was unlikely unless the fourth element, capacity, was present. Fraud diamond theorists utilize the three elements of the fraud triangle theory with the addition of a fourth element – capacity or capability (Huber, 2017; Mangala & Kumari, 2015; Ruankaew, 2016). Capacity or capability refers to the personal skills and ability of the perpetrator to commit the fraud (Boyle et al., 2015; Ruankaew, 2016). Capability

includes the expertise needed to exploit fraud opportunities, the ability to coerce others, and the ability to effectively lie (Boyle et al., 2015).

When investigators analyze fraud, they look closely at the capability or expertise needed to commit the fraud. Expertise, as an element of capability, is when the perpetrator is knowledgeable enough and has the intelligence to exploit internal control weaknesses and to use access to the greatest advantage (Ruankaew, 2016; Wolfe & Hermanson, 2004). People perpetrating identity theft are intelligent and creative with a solid grasp of the various controls and security measures as well as the exploitable vulnerabilities available (Ruankaew, 2016; Wolfe & Hermanson, 2004). Highly intelligent people commit many of the largest frauds (Association of Certified Fraud Examiners Report to the Nation, 2018; Wolfe & Hermanson, 2004).

Perpetrators believe that they orchestrated the fraud perfectly and that the fraud is either untraceable back to them, or that they can easily talk their way out of trouble. Another element of capability or capacity is ego (Wolfe & Hermanson, 2004). The perpetrator must have a strong ego, enough confidence and arrogance to believe investigators will not detect the fraud, or that the perpetrator can easily get out of trouble (Wolfe & Hermanson, 2004). Along with ego is the ability to be very persuasive and able to convince others to commit or conceal the fraud through bullying or threatening (Wolfe & Hermanson, 2004). Related to these elements is the ability to lie to others successfully and convincingly and keeping track of the lies so that the story remains consistent (Wolfe & Hermanson, 2004).

Alternate Theories

Since the advent of computers and the Internet, fraud is one of the highest risk crimes involving a wide range of schemes making detection and prevention essential (Zainal, Som, & Mohamed, 2017). Regardless of the internal controls business leaders have in place, every business and transaction is vulnerable to fraud (Omar, Nawawi, & Salin, 2016). Fraud on businesses affect investors, customers and other stakeholders through decreased revenues and rising costs to consumers (Wood & da Costa, 2015). Evidence of the negative affect exists through substantial increases in insurance premiums or denial of coverage altogether, a decrease in the business' credit rating affecting the business' ability to borrow funds, loss of customer loyalty, and harm to the business' reputation (Amato, 2016). The need exists for leaders to implement both fraud detection and fraud prevention strategies to effectively mitigate fraud (Zainal et al., 2017). Fraud detection is the ability to recognize or discover fraudulent activities, with fraud prevention as the measures taken to avoid or reduce fraud (Baesens, Vlasselaer, & Verbeke, 2015)

The history of fraud theories is extensive, with numerous models authored to explain and aid in detecting fraud. Some of the theories are the fraud triangle by Cressey authored in 1953, power theory by French and Raven authored in 1959, theory of planned behavior by Fishbein and Ajzen authored in 1975, bounded rationality hypothesis by Coleman authored in 1990, fraud diamond by Wolfe and Hermanson authored in 2004, fraud management lifecycle by Wilhelm authored in 2004, organizational fraud triangle by Free, Macintosh, and Stein authored in 2007, crime triangle of routine activity theory

by Felson authored in 2008, the health insurance fraud model by Furlan and Bajec authored in 2008, fraud pentagon by Marks authored in 2009, differential association theory by Gottschalk authored in 2010, neutralization theory by De Bock and Van Kenhove authored in 2011, money, ideology, coercion, and ego or entitlement (MICE) model by Dorminey, Fleming, Kranacher, and Riley authored in 2012, the fraud scale by Mackevicius and Giriunas authored in 2013, opportunity theory by Sen and Borle authored in 2015, first party fraud management framework by Amasiatu and Shah authored in 2018, disposition based fraud model by Raval authored in 2018, and S.C.O.R.E. and S.C.C.O.R.E. fraud models by Vousinas authored in 2019. I discuss these theories in this literature review.

The most popular method of fraud detection is the fraud triangle. Accounting and auditing textbooks, and accounting standards include the fraud triangle exclusively (Free, 2015). In 1953, Cressey formulated a theory regarding fraud that was the basis of the fraud triangle (Abdullahi & Mansor, 2018). There are three interrelated elements of the fraud triangle: perceived need, perceived opportunity, and rationalization (Burke & Sanney, 2018; Lokanan, 2015). Some researchers feel that the fraud triangle is effective because of the enhanced ability of researchers to explain and understand corruption on an individual and institutional level (Maria & Gudono, 2017; Muhtar et al., 2018). However, some researchers feel that the fraud triangle is not thorough enough for business owners and leaders to detect all fraud, thus needs expanding (Boyle et al., 2015; Huber, 2017; Lokanan, 2018; Vousinas, 2019). A fundamental limitation of the fraud triangle is the

lack of clear separation of the attributes of the perpetrator and the circumstances under which the fraud occurs, providing limited insight into the process (Raval, 2018).

Albrecht, Howe, and Romney (1984) developed the fraud scale theory as an alternate to the fraud triangle theory. The fraud scale theory uses the same three elements as the fraud triangle theory with the exception that personal integrity replaces rationalization (Abdullahi & Mansor, 2018). Albrecht et al. theorized that fraud is more likely to occur when the perceived opportunity and perceived incentive or pressure is high, but personal integrity is low. Some scholars feel this change in the fraud triangle, while a step in the right direction, is still not broad enough to cover most fraud adequately.

To overcome the shortcomings of the fraud triangle, Wolfe and Hermanson (2004) expanded the fraud triangle further to include *capability* as the fourth element and dubbed the model *the fraud diamond* (Baker et al., 2016; Mangala & Kumari, 2015; Ruankaew, 2016). Many scholars believed that fraud cannot be committed unless capability is also present, thus supporting the fraud diamond theory (e.g., Boyle et al., 2015; Huber, 2017; Ruankaew, 2016). However, many scholars believed neither the fraud triangle nor the fraud diamond is the answer and proposed other fraud theories (e.g., Amasiatu & Shah, 2018; Eisenberg, 2017; Sen & Borle, 2015).

The fraud triangle is comprised of three elements: perceived need, perceived opportunity, and rationalization. The fraud diamond is an expansion of the fraud triangle, with the addition of *capacity* as the fourth element (Baker et al., 2016). Marks (2009) expanded on the fraud triangle and fraud diamond theories by adding a fifth element –

arrogance – and changing capability to competence, titling this theory the fraud pentagon. According to Marks, while capability and competence mean the same, arrogance is the feeling of superiority the perpetrator feels over others and includes the element of greed. Based on Marks theory, the perpetrator must be competent to perform the fraud. The perpetrator must have the ability or capability to commit the fraud. According to Marks, the perpetrator manifests arrogance and greed through the belief that no one will discover the fraud, or if someone discovers the fraud, the perpetrator will be able to easily get out of trouble. Other scholars did not agree with Marks and presented other theories.

In 1959, French and Raven developed the power theory. The premise was that to commit fraud, the perpetrator influences another to participate whether as a co-conspirator or the victim (Azam, 2018). French and Raven's power theory consists of five elements regarding the perpetrator's power over the co-conspirator or victim, which are reward power, coercive power, expert power, legitimate power, and referent power. Reward power is the perpetrator's ability to provide benefits to the co-conspirator or victim (Azam, 2018). Coercive power is the perpetrator's ability to punish the co-conspirator or victim if the perpetrator's wishes are not complied with (Azam, 2018; French & Raven, 1959). The perpetrator's special power or expertise in a specific area, defined as expert power, is the power the perpetrator needs for the fraud to be successful (Azam, 2018). Legitimate power is the legitimate right the perpetrator has to prescribe or control the co-conspirator or victim's behavior, such as a manger over a worker (Azam, 2018). Referent power is the extent to which the perpetrator identifies with the co-conspirator or victim (Azam, 2018). The power theory works best when collusion or

blackmail is involved in the fraud. Identity theft does not employ these elements; therefore, the power theory does not fit with this study.

With the advent of e-commerce, some theorists considered the traditional fraud triangle and fraud diamond as insufficient models for leaders to determine the risks of data breaches (Sen & Borle, 2015). The opportunity theory of crime and the institutional anomaly theory are models a leader could use to identify factors that can lead to increased risk of data breaches (Sen & Borle, 2015). The basis of the opportunity theory is the assumption that to commit fraud, the perpetrator must have a vulnerable victim (Sen & Borle, 2015). When there is a vulnerable victim, the perpetrator is more likely to behave opportunistically (Sen & Borle, 2015). Sen and Borle (2015) included the institutional anomalie theory in conjunction with the opportunity theory. The basic premise for the institutional anomalie theory is that institutions with strong economic performance are likely to have a greater incidence of data breaches because of the potential for greater riches by the perpetrator (Sen & Borle, 2015). The theories discussed by Sen and Borle remain geared primarily towards e-commerce. However, there are other fraud theories covering a broader spectrum that also include online activities.

A comprehensive fraud theory should include all the factors of fraud for researchers and leaders to develop workable strategies to deter and mitigate fraud. Boyle et al. (2015) felt that simply adding more elements to the fraud triangle was not beneficial. Wilhelm (2004) and other scholars felt excessive focus on detection is unprofitable for businesses and that an antifraud framework that is more comprehensive and broad better serves business' needs (Amasiatu & Shah, 2018). Wilhelm felt the need

for a more holistic approach to fraud management and developed the fraud-management-lifecycle theory based on this belief (Amasiatu & Shah, 2018). The fraud-management-lifecycle theory consists of eight factors, which are deterrence, prevention, detection, mitigation, analysis, policy, investigation, and prosecution (Amasiatu & Shah, 2018). Some scholars felt this framework was too broad and developed an alternate theory.

Using Wilhelm's (2004) fraud-management-lifecycle theory as a base, Furlan and Bajec (2008) formulated the framework for health insurance fraud. The framework for health insurance fraud proposed by Furlan and Bajec consisted of six factors, which were deterrence, prevention, detection, investigation, sanction and redress, and monitoring. The framework for health insurance proposed by Furlan and Bajec does not include the factors mitigation, analysis, policy, and prosecution that are part of Wilhelm's fraud-management-lifecycle theory (Amasiatu & Shah, 2018). Based on the framework for health insurance fraud, the deterrence of fraud starts with removing the reasons for fraud noted in the fraud triangle (Amasiatu & Shah, 2018). Furlan and Bajec stated that there are two business processes; the first is curative involving detection of the fraud, which includes detection, investigation, and sanctioning. The second business process is preventative, which includes detection, investigation, prevention, and sanctioning (Furlan & Bajec, 2008). From the elements of the fraud-management-lifecycle theory and the framework for health insurance fraud, Amasiatu and Shah (2018) proposed a new theory.

Amasiatu and Shah (2018) used elements of the fraud-management-lifecycle theory and the framework for health insurance fraud to formulate the first-party fraud management framework. The first-party fraud management framework consists of seven

factors, which are deterrence, prevention, detection, investigation, sanction and redress, measurement and monitoring, and policy. Amasiatu and Shah contended that their theory is more specific to first-party fraud management and is a theory that business owners could use to develop successful strategies against fraud attacks in a retail environment and through e-commerce. The theory proposed by Amasiatu and Shah is comprehensive, designed specifically for the retail industry. Other scholars disagreed with Amasiatu and Shah, noting that leaders need a broad fraud prevention theory (e.g., Azam, 2018; Baker et al., 2016; Ruankaew, 2016; Sen & Borle, 2015). The ideal fraud theory is one that captures all the elements of a fraud, is workable in all venues, and one that leaders, researchers, and investigators can use to predict, detect, and deter fraud (Azam, 2018; Baker et al., 2016; Ruankaew, 2016; Sen & Borle, 2015). While developing such a comprehensive theory may not be realistic, some scholars believe a broader fraud theory model comes closer than a model tailored for a specific industry or fraud type. To achieve a broader fraud theory model, scholars and investigators proposed several different theories.

One such theory, the differential association theory outlined by Gottschalk (2010), includes the deviant behavior of the perpetrator as learned from peers as an important element. Proponents of the differential association theory noted that long-serving criminal colleagues may influence a new employee by shifting the focus away from the individual to the organization (Eisenberg, 2017). The presence in a business of amoral tone, diffuse responsibilities, and false loyalties create an unhealthy culture that can foster criminal behavior (Eisenberg, 2017). Eisenberg (2017) expanded the differential

association theory, explaining that the perpetrator must reconcile the criminal behavior with societal norms to gain the motivation to commit financial fraud. Eisenberg explained that societal norms are generally *counter-criminal* which means forcing the perpetrator to modify the meaning of the criminal behavior to bridge the gap and reconcile the contradiction. According to the neutralization theory offered by De Bock and Van Kenhove (2011), the perpetrator accomplishes this modification through rationalizing the criminal behavior by using excuses such as entitlement, legal ambiguity, or accepted business practice. Several scholars provided additional insights as to how perpetrators deal with societal norms and the elements that constitute motivation in relation to the various fraud theories that utilize these elements.

The interactionist theory is a theory that also includes societal expectations as a factor in the commission of fraud (Eisenberg, 2017). Proponents of this theory explained that symbols and labels govern all human interactions (Eisenberg, 2017). The perpetrator modifies the perception of these symbols and labels to reconcile the criminal behavior (Eisenberg, 2017). Proponents of the neutralization theory, which also uses societal norms as an element, suggested the perpetrator achieves rationalization using excuses, such as entitlement, legal ambiguity, or accepted business practice (Eisenberg, 2017). Even with rationalizing the fraudulent behavior, motivation must also be present for the fraud to be committed. Most fraud theories include the element of motivation, with each fraud theorist providing additional insights into what motivation is.

Dorminey et al. (2012) defined the perpetrator's motivation through the acronym MICE: money, ideology, coercion, and ego or entitlement. Many of the fraud theories

include the elements of the MICE acronym in one form or another, yet motivation remains present outside of the workplace (McMahon et al., 2016). Proponents of the rational choice theory, which is based on the expected utility model, suggested that the perpetrator can find motivation through the various choices available (Eisenberg, 2017). The basis of both the expected utility model and the rational choice theory is that the perpetrator will choose the option with the greatest utility (Eisenberg, 2017). Unfortunately, these two theories do not take into account emotional distress and the fact that people do not always act rationally (Eisenberg, 2017). Creators of the bounded rationality hypothesis proposed that false assumptions and limited knowledge affect the decisions made by perpetrators (Eisenberg, 2017). Other scholars feel there is yet another factor driving motivation.

Under the bounded rationality hypothesis offered by Coleman (1990), societal structure is the cause for criminal motivation. According to Coleman, the capitalistic culture of competition is responsible for financial crimes. The American dream theory is compatible with Coleman's bounded rationality hypothesis (Eisenberg, 2017). The authors of the American dream theory believed that our excessive preoccupation with monetary success and wealth motivates perpetrators to commit financial crimes when the perception exists that there is no other way to reach these capitalistic cultural goals (Eisenberg, 2017). Some scholars believed that none of these theories completely cover white-collar crime, but cover only distinct elements (e.g., Eisenberg, 2017; Ruankaew, 2016; Sen & Borle, 2015). Perpetrators will always find a way to commit fraud on a victim of which fraud elements are present or not present (Azam, 2018).

The theory of planned behavior, authored by Fishbein and Ajzen (1975), stems from the theory of reasoned action and introduces behavior as an element. The theory of planned behavior consists of four elements: attitude toward the fraud, subjective norms, perceived behavioral control, and moral obligation (Fishbein & Ajzen, 1975). Researchers and investigators use the theory of planned behavior to explain any intentional act or planned fraud by the perpetrator (Raval, 2018). The elements of the theory of planned behavior are somewhat of a replacement of the rationalization element of the fraud triangle; therefore, a means for leaders and fraud experts to explain human behavior (Raval, 2018). Raval (2018) noted that the expansion of the fraud model was insufficient, thus recommending a more accurate and workable theory to include the motivation for action and the motivation for the desire to act. Raval proposed the disposition-based fraud model, which incorporates the perpetrator's character or disposition and the circumstances making up the moral temptation to commit the fraud.

In the theory of disposition-based fraud model, the motivation for action consists of three elements: temptation, intentions, and intentional action (Raval, 2018). Temptation is the violation of the perpetrator's intentions (Fishbein & Ajzen, 1975). Yielding to temptation involves unreasonable revision of a resolve in reaction to outside pressures (Raval, 2018). There are four steps in dealing with temptation: deliberating, judging, choosing, and acting (Raval, 2018). Intention is when the perpetrator resolves to perform an action (Raval, 2018). Intentions are persistent and provide stability to the planned action (Raval, 2018). Deliberating involves the consideration of all available options and the consequences of each option (Raval, 2018). Judging is determining which

option is the best choice and creates belief in the final choice (Raval, 2018). Judging is a critical step in the process because of involving the perpetrator deciding whether to yield to temptation or to resist temptation (Fishbein & Ajzen, 1975). Choosing is where the perpetrator decides intentionally to act on the choice made (Raval, 2018). Finally, acting is when the perpetrator intentionally commits the chosen action and any related actions (Raval, 2018). Raval feels the disposition-based fraud model is an enhancement to the fraud triangle.

Combining the fraud triangle, fraud diamond, fraud scale, and the MICE model to create the new fraud triangle model is a means for auditors and leaders to understand the necessary information to accurately assess fraud risk (Vousinas, 2019). However, Vousinas (2019) argued that the fraud triangle, fraud diamond, fraud scale, and MICE models are incomplete, outdated, and in need of updating. Fraud is constantly changing and evolving; therefore, the need exists for leaders and fraud experts to gain a deeper understanding of why fraud occurs and how to mitigate the effects of the crime (Raval, 2018). The S.C.O.R.E. model includes stimulus, capability, opportunity, rationalization, and ego (Vousinas, 2019). The first four elements of the S.C.O.R.E model emanated from the fraud diamond, with the fifth element added to enhance detection and prevention of fraud (Vousinas, 2019). Ego relates to the perpetrator's feeling of power over other people and situations because of a superior intellect, and is a powerful motivating force (Vousinas, 2019). One of the most common personality traits among fraud perpetrators is ego, evidenced by the drive to succeed at all costs, being self-absorbed and self-confident, and often narcissistic (Vousinas, 2019). Egotists also have a strong need for

admiration while lacking empathy for others, and believe they are superior (Raval, 2018). Ego is the common thread in most white-collar crimes (Vousinas, 2019). Vousinas argued for the expansion of the S.C.O.R.E. model into the fraud hexagon or S.C.C.O.R.E., with the addition of *collusion* as a sixth element. The best use of the S.C.C.O.R.E. model is in conjunction with the original S.C.O.R.E. model, as the two complement each other (Vousinas, 2019).

Mui and Mailley (2015) argued that the fraud triangle theorists considers only the perpetrator and do not consider the environment in which the fraud occurs. The crime triangle of routine activity theory is an expansion of the fraud triangle because of the addition of the target or victim of the fraud and the place of occurrence (Mui & Mailley, 2015). The fraud triangle applies primarily to fraud committed in the United States; some of the elements of the fraud triangle simply do not apply or are not present in other countries (Mui & Mailley, 2015). A need exists for a fraud theory that encompasses the global economy.

Environmental criminologists focus on the fraud itself and the circumstances surrounding the event, providing for a person-situation-interaction view (Mui & Mailley, 2015). Situational crime prevention is the application of environmental criminology with the purpose to decrease crime by increasing the effort and the risk to commit the crime, decreasing any rewards, and removing provocations and excuses that contribute to the commission of the crime (Felson, 2008). The routine activity theory consists of three elements: a motivated perpetrator, a suitable target at a specific time and place, and the

absence of a guardian (Mui & Mailley, 2015). The theory is that a fraud cannot be committed if any one of the elements is not present (Mui & Mailley, 2015).

The crime triangle of routine activity theory (crime triangle) is an expansion of the three elements of the routine activity theory, using three triangles, each addressing the three facets of each element (Mui & Mailley, 2015). The fraud triangle is a subset of the crime triangle. The innermost triangle consists of the three elements necessary for fraud to occur: the potential perpetrator, the victim, or target of the fraud, and the place the crime is to occur (Felson, 2008). The middle triangle represents the supervisors over each element of the inner triangle who could prevent the fraud: the handler supervises the perpetrator, the guardian supervises the target or victim, and the place manager supervises the location of the potential fraud (Mui & Mailley, 2015). The final outer triangle represents the controllers who could regulate the conduct of the elements represented by the middle triangle (Felson, 2008). The crime triangle theory should include crime facilitators (Mui & Mailley, 2015).

Crime facilitators include physical facilitators, social facilitators, and chemical facilitators (Mui & Mailley, 2015). Perpetrators use physical facilitators in the commission of the fraud and to overcome any preventative measures the potential victim has in place (Murphy & Free, 2016). Social facilitators are concepts, such as peer pressure and providing excuses, perpetrators use to help rationalize the fraud act (Mui & Mailley, 2015). Chemical facilitators include drugs and alcohol used to reduce the perpetrator's inhibitions and alter the perpetrator's perceptions of the consequences of the fraud (Mui & Mailley, 2015). The number of facilitators is dependent on the physical

environment and the ability of the perpetrator and one or more facilitators to match up (Mui & Mailley, 2015). Identifying and understanding the role and impact of facilitators is important in designing and developing successful antifraud strategies (Murphy & Free, 2016). The numerous related elements of the crime triangle apply to external fraud threats as well as internal fraud threats at all levels of an organization (Mui & Mailley, 2015). The crime triangle is comprehensive, versatile, and is means for fraud investigators, accountants, and leaders to detect and develop strategies to mitigate numerous types of fraud.

The fraud triangle theory is the dominant fraud theory in use in auditing and forensic accounting textbooks and professional standards worldwide, with the fraud diamond theory considered an excellent complement to the fraud triangle (Mackevicius & Giriunas, 2013; Murphy & Free, 2016). All the fraud theories proposed by scholars, researchers, and investigators began with the formulation of the fraud triangle based on the work of Cressey in 1953. I chose to base my study on the fraud triangle and the fraud diamond theories because these two are the foundation of all other fraud theories and they apply to the parameters of my study, which are to research the effects of identity theft in the hospitality industry and recommend strategies to mitigate the effects of identity theft that are of value to hospitality leaders.

Conclusion

Fraud detection methods are a means for leaders to detect potentially fraudulent transactions, while fraud prevention methods are a means to prevent fraudulent transactions (Mangala & Kumari, 2015). The leaders, managers, and board of directors

are ultimately responsible for the detection and prevention of fraud in their business (Mangala & Kumari, 2015). Despite efforts by businesses in the hospitality industry to detect and mitigate the effects of identity theft, fraud continues to increase in hospitality businesses, with little accuracy regarding the true costs of identity theft (Abdullahi & Mansor, 2018; Bjorke & May, 2016). Effectively detecting and mitigating identity theft is particularly challenging for leaders in the hospitality industry because every transaction, internal and external, is vulnerable to identify theft fraud (Abdullahi & Mansor, 2018; Azam, 2018; Mangala & Kumari, 2015). Chip-enabled credit cards are a means to reduce card-present frauds in the hospitality industry (Carlino, 2018; Froud, 2015). However, with the availability of online and mobile booking in the hospitality industry, card-not-present frauds are increasing in the hospitality industry, as leaders do not know if the they are dealing with a legitimate customer or a fraudster (Carlino, 2018). Due to the intense competition in the hospitality industry and the heightened customer satisfaction requirements, leaders in the hospitality industry use mobile apps to communicate with customers, providing for online booking, offering mobile check-in and check-out services, and providing the ability of the customer to access their room via a mobile app instead of a key card, along with other online and mobile services (Ernst & Young LLP, 2016). Identity theft is a faceless fraud committed easily by fraudsters who often locate in tax havens or territories with no extradition treaty, resulting in significant challenges for authorities to track down the fraudsters and bring them to justice (Compin, 2016). With the hospitality industry allowing customers to make their purchases and reservations

online, the leaders have no way to know who they are really dealing with, resulting in the hospitality industry perceived as enticing for fraudsters.

To combat identity theft fraud, many hospitality leaders implemented strict internal controls, effective corporate governance structures, zero tolerance fraud policies, surveillance strategies and ethical policies to include whistle blower policies, but these strategies and policies are not enough to prevent all instances of fraud (Azam, 2018; Mangala & Kumari, 2015). There is no such thing as the perfect internal control system, so understanding what motivates fraudsters by using the fraud triangle and fraud diamond theories, and heeding *red flags* are the primary tools in detecting fraud (Azam, 2018). Red flags are an indicator of fraud and are present in 92% of fraud cases (Mangala & Kumari, 2015). These red flags are an important facet of early fraud detection (Mangala & Kumari, 2015). Evidence of red flags is present in events and conditions indicating the opportunity for fraud or the actual occurrence of fraud (Mangala & Kumari, 2015). Using the fraud triangle and fraud diamond, the categorization of red flags occurs in numerous ways. Leaders cannot rely on external audits to uncover fraud; hospitality leaders have the responsibility to put effective strategies in place to detect and mitigate fraud and avoid the devastating effect of fraud on their businesses (Kramer, 2015). Implementation of strong fraud detection and mitigation strategies is instrumental in reducing the effect of fraud on hospitality industry organizations (Mangala & Kumari, 2015).

Identity theft fraud is one of the fastest growing global crimes. The need for more research exists on fraud theories, the field of fraud investigation, detection, and mitigation, and the strategies needed by business owners to combat fraud (Golladay,

2017). In 2014, global credit card fraud losses totaled $16.31 billion, or 5.65 cents per $100 of transactions (Kultur & Caglayan, 2017). Future projections indicate that global credit card fraud could exceed $35.54 billion in 2020 (Kultur & Caglayan, 2017). With identity theft fraud affecting the global community, there needs to be a higher level of security and protection strategies involving a partnership between business industries, governments, public institutions, and individuals (Antonescu & Birau, 2015; Froud, 2015). Hospitality leaders attempt to manage a massive volume of information daily and can no longer manually monitor this data for anomalies or fraudulent patterns (Banarescu, 2015). Managing voluminous data requires the use of data analysis tools and programs to aid in identifying anomalies and possible fraudulent activity (Banarescu, 2015). The business industry leverages existing technology to aid in detecting identity theft and preventing fraud through the implementation of the Address Verification System, credit card chip and pin verification, and card verification codes (Carneiro, Figueira, & Costa, 2017). By utilizing an automated fraud detection system, the scanning of all transactions occurs, with any suspicious activity generating an alert transmitted to an investigator for further review (Dal Pozzolo, Boracchi, Caelen, Alippi, & Bontempi, 2018). However, an automated fraud detection system does not indicate every instance of fraud and lacks the capability of indicating if a legitimate credit card presented is one that is actually stolen (Downing, Capriola, & Geller, 2018; Froud, 2015).

Regardless of the size of the business, no business is immune from fraud. Although every fraudulent act is detectable at some point, eliminating all fraud is not possible (Mangala & Kumari, 2015; Omar et al., 2016). The key to effective mitigation of

the effects of fraud is for leaders to take preventative action up front through effective antifraud strategies (Mangala & Kumari, 2015). The proper implementation of effective antifraud strategies reduces the occurrences and impacts of fraud on a business (Mangala & Kumari, 2015). Although larger businesses have the resources to implement elaborate controls and antifraud software programs to detect and mitigate identity theft, there are less expensive effective measures available to small businesses (Kramer, 2015).

To prevent identity theft, the hospitality leader needs to develop strategies that reduce or eliminate the elements of fraud within the constraints of their budget (Alalehto, 2018). The larger hotel and restaurant chains have the resources for expensive and powerful antifraud software programs for utilization companywide effectively mitigating the effects of identity theft within their business structure. One such fraud-detection-software tool is Audit Command Language or ACL (Zainal et al., 2017). ACL has flexibility for leaders and analysts to import large amounts of data in various forms from text, raw data, spreadsheets, and other formats keeping the original data set intact while the user manipulates the data to detect anomalies and trends (Zainal et al., 2017). Unfortunately, this software comes with an expensive annual license fee and all users must attend training sessions, making ACL a viable choice only for larger businesses with significant budgets. Another tool is big data technologies, which are a means for leaders to analyze enormous amounts of data more efficiently and in a shorter amount of time (Zainal et al., 2017). Unfortunately, the big data technologies do not include encryption to protect the data, they are vulnerable to cyber-attacks, and are very expensive to license and train users (Zainal et al., 2017).

Another antifraud software tool is an expert system, which is a computer-based program a cybersecurity expert uses to detect fraud (Zainal et al., 2017). An expert system has a user-friendly interface, is easy to update with new information, and is a means for security analysts to perform real time tests on either new or historical data to assist in investigating potential fraud faster and more efficiently (Zainal et al., 2017). The expert system is also expensive to license and requires users training, making the tool yet another tool available primarily to larger businesses with ample resources dedicated to cybersecurity and antifraud. The expert system is the best technology available for business owners to detect and prevent fraud (Zainal et al., 2017). Leaders have a variety of computer-based tools to mitigate the effect of fraud and identity theft, yet ample evidence in the literature indicate that small business owners are at a disadvantage because of the cost of the software, licensing fees, and required training.

The smaller hospitality businesses, usually found in more rural states with less populated cities and towns, must rely upon less expensive software programs coupled with a better knowledge of their customers and a healthy amount of skepticism. Smaller hospitality businesses know most of their clients by sight, a valuable defense against identity theft in the community, but this alone is not near enough to protect the business from the effects of identity theft. One example of an effective yet inexpensive software tool available to all leaders regardless of budget constraints is Excel (Zainal et al., 2017). The use of an Excel spreadsheet is a means for leaders to identify abnormalities or anomalies, hidden patterns in the data, and provide in-depth analysis of the data to implement the *trust but verify* method (Zainal et al., 2017). While Excel is a valuable tool

for leaders and owners, the software needs supplementing with other antifraud tools (Zainal et al., 2017). An Excel program used in conjunction with card-present transactions can be an effective tool in mitigating the effects of identity theft.

Leaders came together to develop recommendations for data security practices to combat identity theft (Bjorke & May, 2016). Out of this collaborative effort came the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Bjorke & May, 2016). The NIST framework is comprised of five continuous functions for cybersecurity management strategy: identify, protect, detect, respond, and recover (Bjorke & May, 2016). Although no *one size fits all* solution exists for all businesses, commonalities include the need for the continuous collection of cybersecurity risks and incidents, the development and implementation of effective cybersecurity policies, and the regular review of assessments, policies, budgets, response plans, and insurance with revisions made as needed (Bjorke & May, 2016). Businesses were also recommended to ensure that all accounts were set up with the appropriate security clearances, all IT system access is removed at time of termination in real time, and continually update all user accounts deleting those that are not in use, are no longer needed, or belong to employees no longer with the company (Bjorke & May, 2016). Additional recommendations include a review no less than monthly of all accounts for any suspicious activity; implement a system for monitoring user accounts for suspicious activity and utilizing strong passwords and two-step verification; track physical assets such as computers and related devices that must be turned in when an employee leaves the company; mandatory annual cyber security training along with

mandatory password change periods and web filtering to control sites that can be accessed using the company's computers; install and use a strong firewall system; and utilize an intrusion detection system and/or intrusion prevention system (Bjorke & May, 2016). Business owners and leaders could implement these antifraud recommendations and strategies regardless of budgetary constraints for minimal expense to the business.

Transition

In Section 1, I established the foundation of the problem, present the problem statement, the purpose of this study, and the nature of this study. I discussed the use of the fraud triangle and the fraud diamond theory as the conceptual framework for this study. I presented the assumptions, limitations, delimitations related to this study area and discussed the significance of this study to the hospitality industry. In the literature review I discussed the pros and cons of the fraud triangle and the fraud diamond and briefly covered other fraud theories.

In Section 2, I addressed the purpose of this study, outlined my role as researcher, and discuss the protocols I used in selecting study participants. I also included in Section 2 the research method and design, population and sampling, and the means to conduct ethical research. I closed Section 2 with a discussion of the data collection instruments and techniques I used, the data organization techniques and analysis protocols, reliability and validity of the research and findings, and the transition and summary.

In Section 3, I reported the findings and results of my study, provided several recommendations for application in the hospitality industry, and suggested areas needing

further research. In Section 3, I also presented the implications for social change and closed the study with a concluding statement.

Section 2: The Project

In Section 2, I explain my role as the researcher, the eligibility requirements for study participants, my research methodology and design, the population of the study and the sampling method I used, the interviewing process and how I reached data saturation. I discuss what defines ethical research, and how I treated all study participants ethically and kept their information confidential through the data collection process. I outline my procedures for collecting, organizing, and analyzing the data, and the methodology I used to ensure the reliability and validity of the findings.

Purpose Statement

Society benefits when leaders detect consumer identity theft prior to engaging in a business transaction with a fraudulent customer (U.S. Department of Justice, 2016). The purpose of this qualitative multiple case study was to explore the strategies leaders use in the hospitality industry to mitigate the effects of identity theft. The target population consisted of at least five leaders of businesses in the hospitality industry, located in Montana, with successful experience in utilizing strategies to mitigate the effects of identity theft. The implications for positive social change include increased consumer confidence, improved security for consumer data, and reduced consumer financial losses because of identity theft. Society benefits when leaders detect consumer identity theft prior to engaging in a business transaction with a fraudulent customer (U.S. Department of Justice, 2016).

Role of the Researcher

The role of the researcher is to develop the research questions, collect, analyze, and interpret data, and present the findings (Yin, 2018). Researchers should display poise, equality, and be comprehensive in their analysis and interpretation of the data (Leedy & Ormrod, 2015). I was the primary researcher and data collection instrument for this qualitative study. I remained neutral and objective and utilized the data collection and analysis tools available to me to mitigate any bias and to ensure equity in my dealings with all study participants.

Researcher bias is a possibility based on the researcher's past experiences; therefore, the researcher must maintain independence from all other participants (Nagasaka, Bocher, & Krott, 2016). A researcher's background and beliefs may potentially provide bias and skew the research results (Birchall, 2014). I have lived in Montana since 1956 and worked as a regulator in the gaming, bar, and restaurant industry portions of the hospitality industry from 1995 through 2013, dealing with many leaders in the hospitality industry. To mitigate bias in my research, I did not select participants with whom I had a personal or professional relationship.

Reflexivity occurs when the researcher reflects on the ability to remain unbiased while acknowledging the effect of existing bias on the research (Birchall, 2014). I used the reflexive approach throughout the study to mitigate any potential bias. One method to combat bias is using a triangulation strategy that involves the use of multiple data collection methods to provide credibility and validation to the research (Abdalla, Oliveria, Azevedo, & Gonzalez, 2017). To further mitigate researcher bias, I asked open-

ended questions that aligned with the research question, thereby eliminating any unnecessary questions. I used the interview questions to promote a conversation designed to elicit the desired information. After transcribing the responses and engaging the participants in member checking, I compiled the information into a database.

The authors of the Belmont Report summarized the basic ethical principles recommended for researchers (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research [NCPHSBBR], 1979). These principals include respect for the individual participants in the study, beneficence, and justice (NCPHSBBR, 1979). I incorporated these ethical principles into my research using informed consent forms provided to all participants prior to an interview, an assessment of the benefits and risks, and the fair and objective selection of leaders to interview. I used an interview protocol and asked all study participants the same open-ended interview questions in the same order (see Appendix A). Researchers use interview protocol to ensure equal and consistent treatment of all study participants, mitigate researcher bias, and enhance the dependability and credibility of the research data.

The researcher is responsible for ensuring the trustworthiness of the research data (Connelly, 2016). Credibility is the most important part of a case study (Connelly, 2016). Researchers ensure credibility through detailed protocols and believable research claims (Liao & Hitchcock, 2018). To ensure trustworthiness and the credibility of this study, I used member checking with the participants. Researchers establish dependability and confirmability of the research data through analysis, process logs, and detailed notes (Connelly, 2016). To establish dependability and confirmability of the research data, I

performed analysis of data and processes used, and maintained detailed process logs and notes. Researchers ensure transferability and authenticity through a rich detailed description of the study and being transparent about their analysis (Connelly, 2016). I provided transferability and authenticity by including a rich detailed description of this study and the analysis of the data.

Participants

The eligibility criteria for participants in a study must align with the purpose of the study and the research question (Boddy, 2016; Saunders & Townsend, 2016; Yin, 2018). Leaders in the hospitality industry with experience regarding identify theft mitigation strategies consist of business owners, general managers, chief executive officers (CEOs), chief information officers (CIOs), and information technology (IT) leaders (Chong et al., 2017; Roden et al., 2016). The participants in this study were business owners, officers, general managers, or IT leaders in the hospitality industry who had implemented successful strategies to mitigate the effects of identity theft. The research question for this study was: What strategies do some leaders in the hospitality industry use to mitigate the effects of identity theft. The eligibility criteria for participants in this study were as follows: (a) be a leader in the hospitality industry, (b) have successfully implemented strategies to mitigate the effects of identity theft, and (c) lead a company in the state of Montana.

Researchers use purposeful sampling strategies to select study participants (Basta, Tytgat, Klinkenbijl, Fockens, & Smets, 2016; Genel & Topcu, 2016; Meyer, Scarinici, Ryan, & Hickson, 2015; Reeves, 2017). The hospitality industry includes hotels,

restaurants, casinos, bars, theme parks, and movie theaters (Global Hospitality Portal, 2018). I selected one leader from each sector, except for the theme park, to participate.

Current listings of leaders in each hospitality sector were available from the state of Montana Department of Justice – Gambling Control Division statistics for 2018, the Helena Chamber of Commerce, and the Capital Region Telephone Directory (2018). When contacting businesses, I explained the nature and purpose of the study. I provided each confirmed participant a consent form explaining the overall study. Maintaining effective communication with study participants is important in establishing trust and a willingness to participate (Marshall & Rossman, 2016; Yin, 2018). I provided my contact information to all study participants for any questions or concerns.

In a successful qualitative study, the researcher should establish an effective relationship with the study participants (Yin, 2018). Specific procedures should be in place for the interview process, which includes a consent form and set interview protocol to aid in establishing an effective relationship with the study participants (Marshall & Rossman, 2016; Yin, 2018). Researchers foster trust and promote clear and open communication by outlining the specific interview protocol upfront to the study participants (McLevey, 2015). I established an effective relationship with the study participants through in-person and telephone conversations explaining the details of the study along with following a specific interview protocol (see Appendix A) to ensure consistency in the interview process. All study participants received a consent form prior to the interview to ensure a full understanding of the study including my contact information.

Research Method and Design

The proper methodology employed in a study is vital to the success of the researcher (Yin, 2018). I selected a qualitative methodology, multiple case design for this study. The qualitative case study is the most appropriate design for this study because I explored the real-world problem of the effect of identity theft within the bounded contextual setting of businesses in the hospitality industry.

Research Method

Qualitative research embodies a broad range of philosophies, approaches, and methods (Vass, Rigby, & Payne, 2017). Three common research methods exist: qualitative, quantitative, and mixed methods (Turner, Kane, & Jackson, 2015; Yin, 2018). Qualitative research is an inductive approach used by researchers to collect data using open-ended questions and open discourse with participants to gain a deeper understanding of a phenomenon (Gog, 2015). I chose the qualitative research method for this study to gain a better understanding of a specific phenomenon using open-ended questions and open dialog with the participants.

Qualitative research methodology is appropriate when the purpose of the research is to capture the circumstances and conditions of real-world situations (Taylor, Bogdan, & DeVault, 2015; Yin, 2018). In qualitative research, the researcher studies a phenomenon in its natural context and from the perspective of the participants involved in the phenomenon (Vohra, 2014; Yin, 2018). Researchers utilize the qualitative methodology to understand the phenomenon from the participants' perspectives (Berger, 2015). The qualitative research methodology was the most appropriate methodology for

this study because I researched the successful strategies used by hospitality leaders to mitigate the effects of identity theft in their business.

Quantitative research is a deductive approach in which researchers use closed-ended questions and statistics to test hypotheses about the relationships or differences among variables (Barnham, 2016; Gog, 2015; Marshall & Rossman, 2016; Marti, 2016). Quantitative researchers emphasize measurement, testing, and analysis of variables (Makrakis & Kostoulas-Makrakis, 2016). Quantitative research is deductive allowing confirmation of hypothesis, whereas qualitative research is inductive involving the exploration of a phenomenon (Barnham, 2016). The quantitative research methodology was not appropriate because this study does not involve measuring, testing a hypothesis, analyzing variables, or utilizing close-ended questions. In this study, I explored a real-world problem using semistructured interviews and asking participants open-ended questions.

Mixed-method research is a combination of qualitative and quantitative methodologies (Makrakis & Kostoulas-Makrakis, 2016; Yin, 2018). In a mixed-method approach, researchers use a qualitative research methodology in developing a hypothesis with the quantitative research methodology used to test the hypothesis (Jervis & Drake, 2014). The quantitative research methodology was not appropriate for this study because this study does not involve testing a hypothesis. Therefore, the mixed-method approach, which includes utilizing quantitative methodology, was not appropriate for this study.

Research Design

The three qualitative research design methods I considered are: (a) ethnography, (b) phenomenological, and (c) case study. Researchers using an ethnographic design explore the cultural behaviors of participants (Small et al., 2014). Ethnographic research involves the researcher remaining immersed in the culture for an extended period, documenting and getting to know the people being studied, and participating in the study participants' setting (Kaplan, 2016). Researchers also use the ethnography design to study the effect of a society's culture on the behaviors of a select population, and to research the experiences shared by members of that population (Snodgrass et al., 2017). Ethnographic research studies evolve and change based on information researchers gather during the study (Kaplan, 2016). I did not explore the cultural behaviors of participants; therefore, an ethnographic research design was not appropriate for this study.

Phenomenological researchers focus on the shared and lived experiences of participants (Hoi et al., 2013). Researchers using the phenomenological research methodology investigate psychology, consciousness, experience, and behavior emphasizing the research of nature and phenomenon (Song, 2017). Researchers also use phenomenological research to measure how study participants interpret the personal and social world (Hutagalung, 2016). Researchers use the phenomenological research design to study experiences from the participant's point of view (Becker, 2018). The phenomenological design works very well in a mixed-methods study that incorporates quantitative design methods as well as qualitative design methods (Becker, 2018). A phenomenological design was not suitable for this study because I did not collect data

based on the lived experiences of participants and I did not conduct a mixed-methods study.

In a case study research design, researchers explore an activity, process, or event in-depth (Dasgupta, 2015; Yin, 2018). Researchers use a case study design to analyze and develop an in-depth understanding of a phenomenon within a real-world context (Guetterman & Fetters, 2018; Yin, 2018). Researchers use multiple case study research design activities to examine processes or behaviors in their natural settings (Vohra, 2014; Yin, 2018). Researchers use the case study research design when building on or producing new theories, in disputing or challenging an existing theory, to explain a particular situation, to explore or describe a phenomenon, or to provide a basis to apply specific or recommended solutions to a problem or situation (Tumele, 2015). Researchers utilizing the case study research design primarily focus on obtaining answers to *how* and *why* questions (Tumele, 2015). Researchers collect data and explore differences within and between cases through interviews (Dasgupta, 2015). The case study research design works well alone or in a mixed-methods qualitative study and quantitative studies (Guetterman & Fetters, 2018). Multiple case studies increase the robustness of the research findings as compared against single case studies (Vohra, 2014). The case study design was most appropriate for this research study because I explored the real-world problem of the effect of identity theft within the bounded contextual setting of businesses in the hospitality industry. For this study, I chose a multiple case study design because I explored the strategies used to mitigate identity theft by leaders from multiple companies in the hospitality industry.

Data saturation is the point in the research when no new codes or themes emerge from the analysis and interpretation of the collected data (Fusch & Ness, 2015; Hennink, Kaiser, & Marconi, 2017). Data saturation is essential in qualitative research to ensure data sufficiency and validity (Marshall & Rossman, 2016). I recorded the interviews and employed open-ended questions. I also used member checking to ensure the validity of the findings. Researchers use member checking to allow each participant the opportunity to review the researcher's interpretation of their interview data, to ensure accuracy of the information and provide an opportunity to provide additional feedback prior to coding. I conducted five interviews, one from each sector of the hospitality industry. I reached data saturation because during the fifth interview, no new themes, patterns, or information emerged.

Population and Sampling

Defining the Population

The hospitality industry is comprised of five major business sectors, which include bars, casinos, restaurants, hotels and motels, and theaters (Global Hospitality Portal, 2018). In this qualitative multiple case study, the population was comprised of leaders in each of the five major sectors of the hospitality industry. Based on listings from the Chamber of Commerce, various state of Montana agencies, and the regional phone book there are 85 bars and casinos, 121 restaurants, 31 hotels/motels, and two movie theaters for a total population of 239 (Helena Chamber of Commerce, 2018; Montana Department of Justice - Gambling Control Division, 2018; Statewide Publishing-MT, 2018). I included hospitality establishments within Helena, Montana and the immediate

surrounding area. I included businesses qualifying for more than one category in the category most associated with that business and only counted once. For example, two of the hotels also have restaurants but are primarily known as hotels, so I included them in the hotel category. I counted multiple establishments that are under one ownership as one business. For example, I counted two restaurants owned by one person as only one establishment.

Eligibility Criteria

The selected study participants in the sample should include participants that have a significant understanding of the research topic and that can best answer the research question (Marshall & Rossman, 2016). The eligibility criteria must also be in alignment with the purpose of the study and address the research question (Boddy, 2016; Saunders & Townsend, 2016; Yin, 2018). Business owners, general managers, CEOs, CIOs, and IT leaders are the key people in the hospitality industry who are responsible for implementing strategies to mitigate the effects of identity theft (Chong et al., 2017; Roden et al., 2016). The specific eligibility criteria I used in this study was the participant must be a leader in the hospitality industry, such as a business owner, officer, general manager, or IT leader. The next eligibility criteria I used was the participant has implemented the strategies to mitigate the effects of identity theft in the business. The business owners, officers, general managers, and IT leaders meet these eligibility criteria since they are the ones that spearhead the strategies in place for their business and know what works and what has not worked in the past. These leaders are intimately aware of the effects of identity theft on their business. I selected one leader from each hospitality

sector for this study that is knowledgeable of the strategies used to mitigate the effects of identity theft in their business.

Sampling Method

Researchers use purposeful sampling to select study participants based on a strict set of criteria based on the research question (Basta et al., 2016; Genel & Topcu, 2016; Meyer et al., 2015; Reeves, 2017). The targeted population of this study was leaders in hospitality businesses located in Helena, Montana that had successfully implemented strategies to mitigate identity theft in their business. I used purposeful sampling to select one study participant from each category of the hospitality industry, which includes bars, casinos, restaurants, hotels and motels, and theaters. I visited locations from each category and spoke with the leaders to ensure they met the strict eligibility criteria. I explained the nature of the study to each qualifying leader until I had a signed informed consent from one leader from each category for a total sampling of five study participants.

Researchers use convenience sampling to identify study participants based on an existing relationship such as customers of a specific store as opposed to consumers in general (Cheraghalizadeh & Tumer, 2017; Norfara, Koo, & Siti-Nabiha, 2018; Valerio et al., 2016). Convenience sampling was not appropriate for this study, as I selected one leader that meets the strict set of criteria from each of the five sectors in the hospitality industry. Snowball sampling is a chain referral method where initial study participants recruit additional study participants (Valerio et al., 2016). Snowball sampling was not appropriate for this study as I did not depend on initial study participants to recruit

additional study participants. Purposeful sampling was the best choice for this study, as I selected one leader from each of the hospitality industry sectors that met the strict eligibility criteria.

Sample Size

In qualitative studies, researchers concentrate on the richness and quality of the data more than the quantity (Marshall & Rossman, 2016). Researchers use a small sample of no more than 10 to collect rich and in-depth details from the study participants (Yin, 2018). Sample size depends on the scope of the research question and the design of the study (Sim, Saunders, Waterfield, & Kingstone, 2018). Garcia (2018), Saber (2016), and Weiss (2017) all conducted qualitative case studies utilizing purposeful sampling from the local population of leaders meeting their study participant criteria. Both Garcia and Weiss settled on a sample size of three leaders with Saber settling on five leaders. I selected a sample size of five leaders. The sample was comprised of one leader from each hospitality industry sector for a total of five study participants. The sample of five participants was suitable for this study because these leaders were representative of their category in the hospitality industry based on the population.

Interview Setting

The interviewer, anchoring the interview in the purpose of the study and the research question, should utilize an inquiry-based conversation with semistructured open-ended questions and allow for feedback from the study participants (Castillo-Montoya, 2016). Utilizing semistructured open-ended questions ensures the researcher obtains all the information while allowing the study participants the freedom to respond and provide

illustrative concepts (Dasgupta, 2015). The five qualitative data collection methods are interviews, focus groups, document analysis, observation and written questionnaires of which interviews comprise the preferred method 50% of the time (Liao & Hitchcock, 2018). I selected a leader from each sector of the hospitality industry based on the strict set of eligibility criteria previously outlined. I informed the selected study participants of the details of the study prior to the interview utilizing a specific interview protocol (see Appendix A). I held all interviews at the leader's location, or another location of their choosing, utilized semistructured open ended questions with interviews lasting approximately one hour (see Appendix B). I utilized member-checking procedures by recording all interviews and providing each study participant a summary of the interview for review. I allowed the participant to make any changes, corrections, or additions to the summary as needed.

Data Saturation

Data saturation is a core guiding principle in determining sample sizes and reached when the same patterns repeat, and the research obtains no new information and when further coding is no longer feasible (Fusch & Ness, 2015; Hennink et al., 2017; Marshall & Rossman, 2016). Data saturation becomes evident to researchers during the data collection and analysis process (Tran, Porcher, Tran, & Ravaud, 2017). Researchers negatively affect and hamper validity of the research when they do not reach data saturation (Fusch & Ness, 2015). Researchers cannot ascertain reaching data saturation with one interview because there is no basis for determining data saturation until conducting at least two or more interviews (Boddy, 2016). Based on the strict eligibility

criteria noted previously, I selected one leader from each category of the hospitality industry for a total of five interviews. I reached data saturation because during the fifth interview, no new information emerged.

Ethical Research

Researchers must follow ethical standards, which are critical to ensuring the confidentiality and protection of the study participants during the research process (Marshall & Rossman, 2016; Yin, 2018). There are regulatory committees titled Institutional Review Boards (IRBs) in place to oversee standards for human subject research (Blackwood et al., 2015). Researchers must submit the details of their study to IRBs for review and approval prior to involving human subjects in the study. The IRBs have compiled specific criteria researchers must meet (Blackwood et al., 2015). The IRB criteria include minimizing risks to study participants, risk versus benefit, ethical subject selection, the documented voluntary consent of all study participants, and participant confidentiality (Blackwood et al., 2015). The Walden University IRB approval number for this study is 09-11-19-0568616.

Researchers refer to the Belmont Report as a guide in protecting the dignity, privacy, and the freedom of study participants through ensuring the ethical treatment of human subjects in research (Adashi, Walters, & Menikoff, 2018). The three fundamental ethical principles in the Belmont Report are respect for persons, beneficence, and justice (Adashi et al., 2018; Miracle, 2016). To protect study participants, researchers use informed consent and various privacy-protection procedures to ensure confidentiality of the information obtained and the protection of the study participants (Friesen, Kearns,

Redman, & Caplan, 2017). In person-oriented research, there are five practical guideposts researchers should follow: respect for holistic personhood, acknowledgement of lived world, individualization, focus on researcher-participant relationships, and empowerment in decision (Cascio & Racine, 2018).

Holistic personhood is having respect for the study participants and is a cornerstone of research ethics (Cascio & Racine, 2018). Holistic personhood equates to the first ethical principal included in the Belmont report, defined therein as a dual moral requirement to acknowledge autonomy and to protect those with diminished autonomy (Adashi et al., 2018). Researchers utilize informed consent procedures to ensure transparency, compliance with this first principle, and to obtain permission from the participant free of coercion (Adashi et al., 2018; Yin, 2018). Informed consent is a requirement established by federal regulatory agencies to protect study participants and contains details of the study such as the purpose, any associated risks or benefits, terms of compliance, any costs or compensation, and a statement of voluntary involvement and ability to withdraw at any time (Grady, 2015; Hull & Wilson, 2017; Kim & Kim, 2015). I fully explained the nature and purpose of this study to all study participants, provided my contact information, and provided a consent form prior to conducting the interview. The consent form contained the study information explained verbally, my contact information, and instructions on how to opt out of the study at any time. I also explained verbally that the participant may withdraw from the study at any time with no repercussions. Prior to the participant signing the consent form, I clearly conveyed that there will be no compensation paid for their participation.

Acknowledgement of a live world is a companion to the holistic personhood guidepost and refers to the consideration of the impact of past and present external factors that might affect the responses of the participants (Cascio & Racine, 2018). This guidepost closely ties to the Belmont Report's second principle of beneficence (Adashi et al., 2018). To comply with this guideline, the researcher should ensure that the study design is culturally appropriate and not stigmatizing, be forthcoming about any study risks and benefits to the participant and the community, and holding the interview at a location convenient to and comfortable for the participant (Cascio & Racine, 2018). I adhered to this ethical principle through a complete explanation of the study purpose and by allowing the participant to select the best location to hold the interview with minimal interruptions.

Individualization takes into consideration the cultural and social factors that influence study participants without allowing this consideration to overshadow the importance of individual variation (Cascio & Racine, 2018). This guidepost aligns with the third principle of the Belmont Report, which is justice (Adashi et al., 2018). Researcher-participant relationships involve establishing and maintaining trust and rapport between the researcher and study participant (Cascio & Racine, 2018). Qualitative semistructured interviews are by nature flexible allowing for variations between participants and data collection sessions (Cascio & Racine, 2018). This is a qualitative study utilizing semistructured, open-ended questions. I asked all study participants the same interview questions, in the same order, and allowed the study participants to answer to the best of their ability. I recorded and transcribed all interviews

and asked each participant to review the transcript summary of their interview. I provided each study participant the opportunity to make any corrections, changes, or additions they would like. I maintained participant identity confidentiality using a coding system with each participant coded as P1, P2, P3, P4, and P5. I stored all electronic data collected on a password protected external hard drive and stored with all research documents in a locked cabinet. After a period of 5 years, I will destroy all information.

Data Collection Instruments

The researcher is the primary data collection instrument and is responsible for collecting, analyzing, and interpreting data, and presenting the findings (Marshall & Rossman, 2016; Yin, 2018). I was the primary researcher and data collection instrument for this study. Data collection methods researchers use include structured or semistructured interviews, surveys, focus groups, observations, and document reviews (Gog, 2015; Nelson & Cohn, 2015; Yates & Leggett, 2016). The appropriate data collection instruments to use in a study depend on the type of study conducted and the research question (Gog, 2015). I used semistructured interviews and document reviews to collect data (see Appendices A and B).

Interviewees provide a rich account of their experience through interviews that is very difficult to obtain through other data collection methods (Castillo-Montoya, 2016; Nelson & Cohn, 2015). Researchers utilize semistructured interviews when interpersonal contact and opportunities for follow up of specific responses are important and to allow the researcher to deeply explore a specific topic (Nelson & Cohn, 2015; Yates & Leggett, 2016). Recorded and transcribed interviews form the basis for analysis; the interviewer

can take notes and summarize them, or a combination of these methods can be used (Yates & Leggett, 2016). Researchers use open-ended questions to encourage the study participant to relate their knowledge and opinions while the researcher listens and observes (Yates & Leggett, 2016). I used semistructured interviews to allow participants to impart their knowledge and experiences based on the open-ended questions (see Appendix B). Member checking is when the researcher provides a summary of the interview transcript or the interview notes to the participant for review (Birt, Scott, Cavers, Campbell, & Walter, 2016). Qualitative researchers use member checking, also known as respondent validation or participant validation, to verify the data obtained (Birt et al., 2016). With permission of each study participant, I recorded and later transcribed the interview and took detailed notes. I utilized NVivo 12 software to transcribe the recorded interview and provided a copy of the summary of the interview transcription to the study participant for review and to allow for any needed changes, revisions, or additions and to allow the participant to expand on any answers. I then used NVivo 12 to code and analyze the data for specific trends and to determine when I had researched data saturation.

The accuracy and truthfulness of the research findings enhances validity (Cypress, 2017). To ensure validity of the data collected researchers utilize several methods to verify the data obtained to include member checking and document review (Yates & Leggett, 2016). Reviewing documents in addition to semistructured interviews provides additional context and validation to the data obtained (Nelson & Cohn, 2015). In addition to the semistructured interviews, I utilized document reviews. I reviewed the internal

documents that validated the participant's statements such as profit and loss statements, incident reports, policy statements, and insurance claims.

Following a standard set of procedures, or protocols, ensures the dependability and credibility of research findings (Tumele, 2015). Researchers enhance the dependability of their research findings through using the same interview protocols and the same interview questions asked in the same order for each participant (Welch & Piekkari, 2017). I utilized the same interview protocol for each participant and asked the interview questions in the same order for each participant (see Appendices A and B).

Researchers achieve dependability, credibility, and confirmability of the research data through rich thick description, data saturation, member checking, and data coding (Morse, 2015; Welch & Piekkari, 2017). A rich thick description enhances transferability of the study through detailed descriptions of the processes and findings (Liao & Hitchcock, 2018; Morse, 2015). I utilized extensive notes regarding the processes and findings of my study to ensure a rich, thick description and support the prospects of transferability of the finding by future researchers to other cases in other settings.

Member checking involves several steps including transcribing the recorded interview or summarizing the researcher's interpretation of the interview responses and meeting a second time with the study participant (Birt et al., 2016; Liao & Hitchcock, 2018; Morse, 2015). Researchers use member checking to provide the study participant the opportunity to review the summary information compiled by the researcher and make any needed changes or revisions, and additionally provides the researcher the opportunity to ask if there is any additional information the participant would like to add (Birt et al.,

2016; Liao & Hitchcock, 2018; Morse, 2015). I used member checking to ensure the accuracy and completeness of the data collected and to determine data saturation.

Data Collection Technique

Researchers use several data collection techniques, which include semistructured interviews, member checking, and document reviews to ensure the dependability and accuracy of the data obtained (Dasgupta, 2015; Morse, 2015). Researchers obtain case study data primarily through semistructured interviews to allow the participants ample time to fully respond to each question (Dasgupta, 2015). The researcher follows up with member checking to confirm the data (Morse, 2015; Welch & Piekkari, 2017). Researchers utilize data coding to aid in data analysis and ensure data saturation (Clark & Veale, 2018; Liao & Hitchcock, 2018; Morse, 2015). As the primary researcher, I used semistructured interviews to obtain rich descriptions from study participants regarding their experience with mitigating the effect of identity theft in their business. I used member checking to ensure that my interpretation of the information imparted to me was accurate and complete. I also used document reviews to collect additional study data and to verify the information obtained through the interview and member checking processes.

Proponents for semistructured interviews argue that researchers use semistructured interviews to ask open-ended questions, to ask follow-up questions for clarification purposes, and to obtain a rich and detailed account of the participant's experience that is difficult to obtain through other methods (Castillo-Montoya, 2016; Nelson & Cohn, 2015). Opponents of semistructured interviews argued that the data obtained is subjective, unverifiable, and that interpretations of the data lend themselves to

researcher bias (Barnham, 2016; Cope, 2014). To overcome the perceived flaws in semistructured interviews and to enhance the dependability of the data, researchers use interview protocols, member checking, and triangulation (Barnham, 2016; Cope, 2014).

Researchers use triangulation to expand the understanding of the data and provide authentication of the data obtained by using information collected from multiple sources (Morse, 2015; Welch & Piekkari, 2017). Triangulation is a means for researchers to use data obtained from multiple sources to authenticate or validate the data (Morse, 2015; Welch & Piekkari, 2017). Methodological triangulation occurs when researchers use more than one method to verify data (Tibben, 2015). An example of method triangulation is using semistructured interviews along with document review to verify the data obtained (Tibben, 2015). Reviewing documents related to the information obtained through the interview process provides a context for further evaluation and aids in triangulating the findings (Nelson & Cohn, 2015). A limitation of using document review is that the researcher may not know exactly what documents to review, the documents may be difficult to access, and may not provide enough context to be useful for evaluation purposes (Nelson & Cohn, 2015). Opponents further argued that triangulation is akin to conducting the research study twice, is time consuming, and the research gains little in the process (Kilinc & Firat, 2017; Morse, 2015; Tarin, 2017).

The interview protocol is a tool that researchers use to obtain information specific to the aims of the study and to encourage a conversation about a specific topic (Castillo-Montoya, 2016). I used a specific interview protocol (see Appendix A). I interviewed one leader from each sector of the hospitality industry. I introduced myself and explained that

I am a student at Walden University conducting a qualitative study on the successful strategies leaders in the hospitality industry use to mitigate the effects of identity theft. I conveyed to each participant that the published study will not contain any personally identifiable information and that I will destroy all research records after 5 years. I provided each participant a consent form prior to the interview and explained that they can elect to opt out at any time. Once the participant consented to the interview, I conducted a semistructured interview lasting approximately one hour. I followed the interview protocol and used the same interview questions, asked in the same order for all participants, took detailed notes and record the interviews to ensure accuracy of the data, and used reflective journaling to mitigate personal bias (see Appendix B). Participants had the opportunity to ask questions before, during, and after the interview.

Researchers use triangulation to obtain richer, fuller data and to help verify the data (Wilson, 2016). Triangulation involves using more than one source of data (Wilson, 2016). I verified the interview data collected from each study participant by reviewing additional company reports and documents. I reviewed various company documents specifically related to the effects of identity theft in their hospitality business, such as incident reports, insurance claims, recorded revenue losses, written policy statements, and the results of the strategies used to mitigate the effects of identity theft to validate the data obtained through the semistructured interview.

Researchers use member checking to allow the participants to verify the accuracy of the researcher's notes or the summary of the transcribed interview and clarify or expand on any of their answers (Birt et al., 2016; Dasgupta, 2015). Opponents of member

checking pointed out that the participants have too much latitude to make changes, additions or deletions requiring the researcher to reanalyze the data especially if the researcher synthesizes data with data obtained from other participants (Morse, 2015). The need to reanalyze the data is very time consuming on the part of the researcher (Morse, 2015). Opponents also stated that member checking can hinder the free flow of information from the participant to please the perceived needs of the researcher (Morse, 2015). I transcribed each recorded interview and typed up a summary of the detailed notes taken during the interview. I provided each participant the opportunity to review a summary of the initial interview summary and allowed the participant to make any corrections or additions, or to add to or expand on any responses. I additionally included a short follow-up interview at the same time to ensure the participant the opportunity to provide all available information, and to ask any additional questions. During the follow-up interview, I specifically asked the participant if the summary of the initial interview was accurate and if there was any additional information they wanted to add. After the participant reviewed and approved the summary of the initial interview, I coded and synthesized the information into the other data collected. Utilizing member checking helped to ensure the accuracy and dependability of the data prior to coding.

Researchers use pilot case studies for larger studies to test and refine the methodology, assess the effectiveness of the methodologies employed (Henson & Jeffrey, 2016; Yin, 2018). Researchers use pilot studies for much broader studies and are not appropriate for this study. The limited scope of my study did not warrant the use of a pilot study.

Data Organization Technique

Researchers use data organization to aid in analyzing information, support the findings, and protect the participants' confidentiality (Bernard, Wutich, & Ryan, 2016; Yin, 2018). I utilized NVivo 12 data analytic software to aid in my data organization. NVivo software automatically codes audio clips with no prior transcription needed based on the research question and allows the codifying of information several different ways without modifying the original data (Oliveria, Bitencourt, dos Santos, & Teixeira, 2016). Researchers can also use NVivo to include any notes, comments, or reminders in a memo section and is fully compatible with Microsoft Excel and Word (Oliveria et al., 2016). I recorded and transcribe all interviews using the transcription features available through NVivo 12, which automatically transferred the data to the main NVivo 12 software module for coding. I organized the additional data from my notes and document reviews in an Excel workbook. I then transferred the data into NVivo 12. I used the features of NVivo 12 data analysis software to mitigate any bias I had towards the data, to recognize themes and trends, and determine when I reached data saturation.

Researchers use reflective journaling to help evaluate any biases and preconceptions that exist and aide in avoiding manipulating the study's findings and conclusions (Peters & Halcomb, 2015; Yin, 2018). Prior to beginning the interview process, I used reflective journaling to recognize any biases or preconceptions I may have had.

A generic identification code assigned to each participant aids in ensuring the confidentiality of the participant's personally identifiable information (Johnson, 2015).

The IRB is responsible for ensuring the rights, dignity, well-being, and safety of the research participants, and that researchers do not violate these rights (Sherchand, 2017). To ensure these rights, the IRB have developed specific rules and regulations that researchers must follow (Murtha & Lipkin, 2017). To ensure the protection of participants', and in keeping with the IRB requirements, I utilized a generic system that does not refer to the participant, such as P1, P2, P3, P4, and P5, and used this coding system when conducting all interviews and document reviews. I used this coding convention on all electronically stored data, transcripts, and notes. I stored all electronic data on an external password protected portable hard drive. I will retain the password protected portable hard drive, notes, and other documentation in a locked cabinet for a period of 5 years, after which I will shred all documentation, and erase all electronic files from the portable hard drive.

Data Analysis

According to Yin (2018), researchers should follow five steps when analyzing data. The five steps include (a) compiling data, (b) dissembling data, (c) reassembling data, (d) interpreting data, and (e) reaching conclusions (Yin, 2018). By utilizing and analyzing data from various sources, researchers can address a wide range of subjects while providing validity to the research study (Yin, 2018). I used Yin's five-step data analysis process of compiling, disassembling, reassembling, interpreting, and in reaching conclusions based on the data. I utilized Microsoft Excel and Word to help compile the data and identify patterns for the coding process (dissembling). Coding the data utilizing NVivo Pro 12 software aided in recognizing common themes (reassembling). I analyzed

the common themes against the data obtain from various other sources (interpreting the data) using methodological triangulation and compared the results to my conceptual framework and the published literature (reaching conclusions).

Methodological triangulation is the most common type of triangulation researchers use to compare interview data, organizational documents, and published literature to enhance the researcher's conclusions (Joslin & Muller, 2016; Wilson, 2016). Researchers using methodological triangulation incorporate data from multiple sources to provide a more complete picture of the phenomenon (Drouin, Stewart, & Van Gorder, 2015). In this qualitative research study, I used methodological triangulation during data analysis by utilizing semistructured interview questions that align with the central research question, field notes, company documentation, and reflective journaling. I also analyzed the recorded interviews to recognize and aid in categorizing the evident themes and patterns that emerged regarding the strategies used to mitigate the effects of identity theft in the hospitality business. I used methodological triangulation to compare the data collected against published literature and my conceptual framework to enhance data validity, ensure the dependability of the data collected, and the credibility of my research findings.

Compiling

Compilation of data occurs through conducting face-to-face interviews using an interview protocol and taking notes, reviewing company documents, observational data, and transcribing and coding each interview (Yin, 2018). I conducted face-to-face semistructured interviews, took extensive notes, and reviewed available company

documents. I compiled the interviews, notes, and related summaries using a combination of Microsoft Excel, Word and NVivo Pro 12 software. I input the data obtained from the interviews, notes, and document reviews into an Excel spreadsheet and prepared it for coding. I utilized NVivo Pro 12 software to capture the main ideas and to detect themes, and to code the data. Researchers use data coding with semistructured interviews to aid in determining data saturation and to aid in data analysis by capturing the main ideas or themes in the data collected (Clark & Veale, 2018; Liao & Hitchcock, 2018; Morse, 2015). By using a coding process, researchers can interpret the information from participant interview to broader themes (Bernard et al., 2016). Data saturation is the point at which no new information or themes are forthcoming from the data collection process (Boddy, 2016; Fusch & Ness, 2015; Hennink et al., 2017).

Disassembling

Researchers provide a detailed discussion of the coding process by describing the data processing steps, the disassembly into meaningful fragments, ordering the meaningful fragments into new fragments of analogous meaning, and a description of the underlying categories (Kohler, 2016; Yin, 2018). The disassembled data fragments become part of a subset of codes, categories and themes that are most used by researchers that aid in understanding the data (Firmin, Bonfils, Luther, Minor, & Salyers, 2017; Yin, 2018). I utilized a generic coding system with participants assigned a code such as P1, P2, P3, P4, and P5 for each participant interviewed. I separated all data received through the face-to-face structured interviews, notes, and company documents into core and

subcore themes using Microsoft Excel for input into NVivo Pro 12 software. I utilized NVivo Pro 12 software for further data analysis.

Reassembling the Data

Data coding helps the researcher to determine data saturation and to aid in data analysis by capturing the main ideas or themes in the data collected (Clark & Veale, 2018; Liao & Hitchcock, 2018; Morse, 2015). Data analysis software aids in ensuring dependability and confirmability of the data, and helps mitigate researcher bias (Davidson, Thompson, & Harris, 2017; Oliveria et al., 2016; Paulus & Bennett, 2017). While data analysis software is a great help in data analysis, the researcher is still responsible for creating the codes, determining the association between a given code and the data, deciding which codes belong to which categories (Davidson et al., 2017; Oliveria et al., 2016). After verifying the data, I coded the information and utilized NVivo Pro 12 data analysis software to analyze the data obtained and to determine when I reached data saturation based on the results provided.

Interpreting Data

Researchers enter the research information gathered into NVivo software and the software codes the information based on the research question (Oliveria et al., 2016). This software will also automatically code audio clips with no transcription needed (Oliveria et al., 2016). Researchers can codify information several different ways without modifying the original information (Oliveria et al., 2016). This software also allows the researcher to include notes, comments, and reminders in the memo section (Oliveria et al., 2016). NVivo is compatible with Excel and Word (Oliveria et al., 2016). NVivo Plus

software could be helpful for a reaching conducting social network analysis, pattern-based auto coding, automated insights, egocentric sociograms, network sociogram, and social media sociograms. The use of the many features and the flexibility of the NVivo Plus software enabled me to efficiently categorize and interpret the data and compare the patterns and themes to the primary and secondary data and to the purpose of this study.

Concluding Data

Qualitative research should be transparent, well supported, reflexive, ethical, have a clear theoretical background, and contribute to existing theory (Cavalcanti, 2017). Using multiple research methods is a means for researchers to contribute to validity, mitigate bias, and draw conclusions (Abdalla et al., 2017). In the final phase of the research study, the researcher draws conclusions from the data and reports the findings (Yin, 2018). Researchers use the information from the interpretation phase as the basis for the conclusions (Yin, 2018). I drew my conclusions from information obtained from the interpretation phase, the research question, the conceptual framework of the study, and the existing literature.

Software Plan

The three primary data software packages used in qualitative data analysis are ATLAS.ti, MAXQDA, and NVivo. While data analysis software is a great help in data analysis, the researcher is still responsible for creating the codes, determining the association between a given code and the data, deciding which codes belong to which categories (Davidson et al., 2017; Oliveria et al., 2016).

Researchers use ATLAS.ti software as a project management tool, for literature reviews, transcription, and data analysis (Paulus & Bennett, 2017). ATLAS.ti is currently compatible with Mac desktop and Windows desktop and has a cloud version and mobile apps available for Android and iPad systems (Paulus & Bennett, 2017). ATLAS.ti provides excellent support but is not easy to learn and it takes considerable time for users to become proficient in using the software (Paulus & Bennett, 2017). Currently features like transcription, document editing, A-Docs, the ability to print documents with margins, or relative values in code-doc table features are not available.

MAXQDA consists of four windows: data from the project, a document system, the codes and categories, and a document browser (Oliveria et al., 2016). Researchers can create codes before, during, or after data analysis with the codes presented in a tree structure (Oliveria et al., 2016). The MAXQDA software allows the user to delete, edit, or reclassify the codes without losing any content previously examined (Oliveria et al., 2016). The coding system can be color coded and reminders included for clarification (Oliveria et al., 2016). MAXQDA is also compatible with Excel and HTML formats for downloading information (Oliveria et al., 2016). MAXQDA software offers analysis tools for mixed methods, statistical, and quantitative content, and is compatible with both Mac and Windows. They offer several products including MAXQDA Standard, Plus, and Analytics Pro and have mobile apps for Android and iOS. They also provide training courses, seminars, and blogs.

NVivo is available for both Mac and Windows users. NVivo 12 for Windows is the current version with NVivo Pro and NVivo Plus. Training, webinars, a free online

guide for beginners, and various guides are available to the user and a free download of NVivo 11 is available. A free trial of NVivo Transcription is also available.

The MAXQDA and NVivo software packages are very similar with the main differences in nomenclature used and their interface (Oliveria et al., 2016). The preference is solely up to the researcher. For this qualitative multiple case study, I selected the NVivo 12 Pro software as it best fits the small amount of data I worked with. I did not need the availability of mobile apps or quantitative analysis tools that are available with MAXQDA and ATLAS.ti for this study. However, I did use the transcription package as it was extremely helpful when transcribing the interviews.

Key Themes

Researchers use the major themes that emerge from the research data to support and provide additional understanding of the conceptual framework of the study and the relevant published literature on the subject (Unkovic, Sen, & Quinn, 2016). The use of data analysis software aids in ensuring credibility, dependability, confirmability, transparency, and helps in mitigating researcher bias (Davidson et al., 2017; Oliveria et al., 2016; Paulus & Bennett, 2017). I used the conceptual framework and published literature to support, verify, and contextualize the key themes that emerged from data obtained through interviews and document reviews, and using the NVivo Pro 12 software.

Reliability and Validity

Reliability and validity are key aspects of all research, both qualitative and quantitative, and are necessary components of quality research (Cypress, 2017). In a

quantitative method study, the researcher uses numeric and empirical data to test hypotheses and validate results (Marshall & Rossman, 2016). Researchers conducting qualitative studies rely on nonnumeric data to support their research findings (Yin, 2018). Guba and Lincoln (1989) introduced criteria for determining trustworthiness, or rigor, of qualitative research. Guba and Lincoln replaced the terminology for achieving rigor to trustworthiness, and from reliability, validity, and generalizability with the terms *dependability*, *credibility*, and *transferability* (Morse, 2015). Researchers consider credibility as one of the essential indicators for a strong qualitative study (Liao & Hitchcock, 2018).

Dependability

To ensure dependability of the study, researchers seek factors such as the stability of the data over time, the study conditions, and consistency of the findings (Amankwaa, 2016; Connelly, 2016). Researchers establish consistency through the transparency of the research practices, the analysis of the data obtained, and the conclusions rendered (Cypress, 2017). Dependability occurs when other researchers can obtain consistent results using similar processes in similar settings (Kornbluh, 2015). Maintaining a detailed audit trail of the decisions made throughout the research process ensures dependability (Baillie, 2015). Extensive journaling of all stages of the research including all decisions and the thinking behind the decisions provides a detailed audit trail (Baillie, 2015). I maintained an extensive journal of every step of the research process to include my decision-making process and the thinking behind each decision made. I followed a set interview protocol with each participant. I used member checking to ensure accuracy of

the information recorded along with a review of related financial documents. I continued participant interviews until I reached data saturation.

Credibility

Confidence in the study and the findings by others and is the most important criterion (Connelly, 2016). Researchers use credibility techniques to help assess the veracity of data and conclusions and include the attributes of accuracy and accountability (Liao & Hitchcock, 2018). Credibility techniques include prolonged engagement with participants, interview protocol, observation, detailed notes and journaling, triangulation of data, and participant member checking (Baillie, 2015; Connelly, 2016; Morse, 2015). To ensure credibility, I used the same interview protocol with each study participant, made notes of all observations, utilized extensive journaling of the data collection and decision-making process, utilized triangulation of data through the review of related company documents, and used participant member checking. I also used NVivo Pro 12 software to further document the data process and aid in mitigating any researcher bias.

Confirmability

Confirmability is the degree findings are consistent and another researcher could replicate the study (Connelly, 2016). Researchers establish confirmability using triangulation strategies to ensure objectivity in the research (Morse, 2015). The researcher can also ensure confirmability through reflective journals kept through the research process (Baillie, 2015). I used reviews of related company documents, such as insurance reports and revenue reports, member checking, and extensive journaling of each step of the research process and every decision to ensure confirmability of my

findings. I documented all procedures in detail so that future researchers might replicate my study. I documented all findings, clearly noting any discrepancies or anomalies in the findings that may indicate areas that need further study.

Transferability

Using thick, rich descriptions in a study is a means for researchers to enhance transferability by providing other researchers the ability to use the original findings in another context (Baillie, 2015; Connelly, 2016; Morse, 2015). By using thick, rich descriptions, the original researcher provides a sufficiently detailed description of the research to enable future researchers to determine if the research findings are transferable to other contexts (Baillie, 2015). By utilizing rich, thick descriptive journaling, I provided the information needed for future researchers to determine the transferability of the study.

Researchers use data triangulation to enhance the validity of the findings, which aids in transferability of the research (Abdalla et al., 2017). By utilizing triangulation methodology researchers reduce the risk of impaired findings due to shortcomings and limitations and produces more credible conclusions (Abdalla et al., 2017). Researchers use triangulation methodology to corroborate findings and test validity (Amankwaa, 2016). I utilized triangulation methodology to ensure credible, dependable, and trustworthy findings.

Another methodology a researcher may use to validate findings is data saturation. Researchers reach data saturation when no new information or themes are forthcoming from the data (Boddy, 2016). In qualitative research studies, researchers use coding to analyze the data collected and to identify recurring themes or patterns (Clark & Veale,

2018). I determined the point of data saturation in my study using Microsoft Excel and NVivo 12 software.

Data Saturation

Researchers attain data saturation when additional data obtained yields no new codes or themes (Boddy, 2016; Fusch & Ness, 2015; Hennink et al., 2017). Data saturation is essential in qualitative research to ensure data sufficiency and validity (Marshall & Rossman, 2016). Failure of a researcher to reach data saturation affects the quality of the research and hampers validity (Fusch & Ness, 2015). The total number of interviews required to reach data saturation is dependent on the research study and not a hard and fast number (Fusch & Ness, 2015). Due to the limited size of the population, I initially conducted five interviews, one from each sector of the hospitality industry. I utilized the full features of the NVivo Pro 12 software to help in determining when I reached data saturation or if the need existed to conduct additional interviews. No new themes or patterns emerged during the fifth interview; therefore, I reach data saturation.

Transition and Summary

In Section 2, I outlined details of the research project designed for my exploration of strategies leaders use to mitigate the effects of identity theft in the hospitality industry. Section 2 of this study included the role of the researcher, the research method and design, population and sampling protocols, data collection, data organization and analysis techniques I used, and methods to establish reliability and validity of the study. I described the processes I used to ensure dependability, credibility, transferability, and confirmability which supports the reliability and validity of my research findings. In

Section 3, I present the study's findings, the application for professional practice, implications for social change, my recommendations for action and areas of further research, my reflections, and the study's conclusion.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the strategies business leaders use in the hospitality industry to mitigate the effects of identity theft. I collected the data in this study through semistructured interviews with five business leaders in the hospitality industry who successfully implemented strategies to mitigate the effects of identity theft in their business. To enhance the accuracy of the data collected, I engaged the participants in member checking and used methodological triangulation by reviewing company documents and published literature in this field to validate the interview data. The company documents reviewed included written policies and procedures, comparative profit and loss statements, employee training manuals, and educational flyers to customers. The themes that emerged were (a) a new technology strategy, (b) a training and educating strategy, and (c) a vigilance strategy. This section of the study contains the presentation of the findings, applications to professional practice, implications for social change, recommendations for action, recommendations for future research, reflections, and the conclusion.

Presentation of the Findings

The research question addressed in the presentation of the findings is: What strategies do some leaders in the hospitality industry use to mitigate the effects of identity theft? The targeted population for this study was business leaders in the hospitality industry in Montana with experience regarding successful identity theft mitigation strategies. I used purposeful sampling to identify five participants who met the eligibility

criteria to take part in this study. I collected data through semistructured interviews, member checking, and a review of company documents, continuing until no new themes or patterns emerged. I used the code names of P1, P2, P3, P4, and P5 to protect the confidentiality and privacy of the study participants. The conceptual framework used in this study was a combination of the fraud triangle theory by Cressey (1953) and the fraud diamond theory by Wolfe and Hermanson (2004), who built upon the fraud triangle theory. I used Yin's (2018) five-step data analysis process, which consists of compiling the data, disassembling the data, reassembling the data, interpreting the meaning of the data, and concluding the data to analyze the data collected. I used Microsoft Excel and NVivo 12 Pro software to analyze the emerging themes and patterns based on the data collected, and to verify when data saturation occurred.

Participation by all study participants was voluntary. I obtained a signed consent form prior to each initial interview. I was able to conduct three face-to-face interviews and two telephonic interviews each lasting approximately 30 minutes, with an additional follow-up interview averaging approximately 20 minutes per participant to allow for member checking and additional data gathering. I obtained access to various company documents with permission of the participants. I utilized methodological triangulation along with member checking to ensure I reached data saturation and to ensure dependable, credible, confirmable, and trustworthy findings. I used Microsoft Excel and Word when transcribing the interviews and related notes, and then uploaded the transcribed information into NVivo 12 Pro to organize and analyze the data into themes.

The three themes that emerged from the data analysis were (a) a new technology strategy, (b) a training and education strategy, and (c) a vigilance strategy. Table 1 is a display of the emergent themes and percentage use by the business owners that participated in this study. The themes developed aligned with the conceptual framework and literature review as provided in Section 1 of this study.

Table 1

Mitigation Strategies

Strategy	Percent of Use by Owners
New Technology Strategy	80%
Training and education Strategy	100%
Vigilance Strategy	100%

Theme 1: New Technology Strategy

The first theme that emerged, and was present throughout all five interviews, was the use of new information security technology. All five participants spoke to the need to secure sensitive business and customer information, however, only P1, P3, and P5 had instituted advanced security technology measures. P2 and P4 chose a less advanced security protocol for their businesses. P1, P3, and P5 chose to utilize an off-site, third-party, secure local area network (LAN) server with extremely limited access to store all sensitive business and customer information citing the ability to more efficiently limit access to the information thereby making the information stored more secure. P1 and P3 elected to eliminate all paper records, relying on the secure electronic records only. P5 opted for a combination of a third-party secure server for sensitive information storage

along with continued retention of select information on paper and stored in a locked file cabinet. P2 and P4, while agreeing on the need for strict security measures, utilized only electronic check authorization, and maintained paper copies of sensitive information stored under lock and key. Table 2 is a display of the various successful tactics used by the participants to implement their new technology strategy.

Table 2

Tactics Used to Implement New Technology Strategy

Tactic	Percent of Use by Owners
Off-site third-party secure LAN server	80%
Electronic information storage only	60%
On-site automatic information security system	20%
Paper documentation in secured storage	20%

P1 stated, "We conducted extensive research prior to committing to an off-site secure LAN server." Comments by P3 and P5 aligned with comments from P1 regarding the added security of moving the secured LAN server off-site. P1, P3, and P5 commented that the off-site LAN server allowed them to better secure the information as well as providing the ability to further restrict access to the information. I verified these statements through a review of the documentation provided by the third-party LAN providers outlining the customizable services and security protocols available to their customers. I also verified the statements through written memos and updated policy statements documenting the research and decision-making process by P1, P3, and P5.

P1 and P3 both chose to transition from paper retention of sensitive information to secure electronic storage. Both participants cited the increased ability to secure both

business and customer information through more limited access to the off-site LAN server. P1 felt this move significantly reduced the ability of employees to access sensitive business and customer information. P3 commented, “Sensitive business and customer information was more secure, easier to limit and monitor access to the information, and vulnerability to the theft or misuse of sensitive information was greatly reduced by converting to strictly an electronic storage platform.” I verified these statements through a review of written policy and procedures manuals and employee manuals. The manuals contained a section that clearly outlined that all information was to be in electronic format and that the creation and retention of paper copies has been discontinued. The manuals also contained statements regarding the limited access of electronic information to select upper management personnel only.

P2 and P4 preferred to use on-site automatic information security systems. Both cited they felt the information was easier for them to control and more convenient for both the employees and customers. P4 stated, “The transition to the automatic information security system drastically reduced returned checks and charge backs along with claims of stolen check books and credit cards thus increasing revenues.” P2 used an automated information security system for several years and experienced the same reduction in returned checks, charge backs and revenue increases as P4. In 2019, P2 transitioned away from the automatic information security system to a cash only system, which P2 stated, “even more dramatically increased revenues and eliminated the need to collect or retain sensitive customer information.” I verified the statements made by P2 and P4 through reviews of their annual consolidated profit and loss statements covering

the periods prior to and after the implementation of the automated information security systems. I additionally reviewed a comparison of the annual consolidated profit and loss statements for P2 for the periods the automated information security system was in use and after implementation of the cash only system. The documents reviewed aligned with statements made by P2 and P4 reflecting significant increases in revenues coupled with a substantial decrease in returned checks and charge backs.

P2 and P4 were the only participants to continue to use a paper-based information retention system with the information kept in a locked cabinet with restricted access. While P4 continued to retain both sensitive business and customer information in paper format, P2 retained only sensitive business information. P2 and P4 felt these procedures allowed them increased flexibility without being dependent on the Internet or computer system and protected the information from loss due to a system failure. P4 stated, “I cannot allow my business to be at risk for a computer crash or an Internet hacker; that is why I keep paper records of everything.” Both P2 and P4 felt the policies implemented regarding the security of sensitive information were enough for their business. I verified this information through a review of memos, meeting minutes, and written policies that contained clear statements about the location of the stored information, that the cabinet must remain locked, and who has access to the information.

The findings regarding the implementation of new information security technology to secure the sensitive information of both businesses and customers aligns with the fraud triangle and fraud diamond theories because, as noted by both Cressey (1953) and Wolfe and Hermanson (2004), business owners and leaders need to utilize

new technologies in their fight against the effects of fraud in their businesses. These two fraud theories, when used together, aid business leaders in understanding how fraud occurs, what conditions are conducive to fraud, and the mindset behind fraud. Armed with this understanding, business leaders are in a much better position to determine the appropriate information security strategies specific to their business.

According to the existing literature, the hospitality industry remains affected by identity theft through the loss of revenue, reduced confidence in the business by the customer, and increased costs to both customers and affected businesses due to hidden costs related to identity theft all totaling hundreds of billions annually (Amato, 2016; Antonescu & Birau, 2015; Chong et al., 2017). The findings of a new technology strategy confirmed the research of Kauspadiene, Ramanauskaite, and Cenys (2019) who noted that business owners must use the most current and efficient systems to effectively mitigate the effects of identity theft. The findings also confirmed the research by Cram, D'Arcy, and Proudfoot (2019) in that the ability of businesses to secure sensitive business and customer information is essential to the ongoing success of all businesses in today's technology driven global economy. The findings reflected by the increased revenues coupled with the financial and economic stability of the participants after instituting information security strategies further confirmed the research conducted Cram et al. and Kauspadiene et al. Business owners must do the research and remain fully informed to be able to determine the strategies needed to ensure the confidentiality, integrity, and security of sensitive business and customer information (Flowerday & Tuyikeze, 2016). Armed with this knowledge, along with the latest in information security technology,

business leaders have the tools to successfully mitigate identity theft in their businesses. However, all the participants pointed out in the interviews that business leaders must institute ongoing training and remain vigilant and able to update strategies as needed.

Theme 2: Training and Education Strategy

The second theme that emerged was a training and education strategy. P1, P2, P3, P4, and P5 noted the importance of training employees and educating the customers on the new policies and procedures. Statements by P1, P3 and P5 were consistent with the belief that initial and ongoing training of employees was key to the acceptance of and compliance with the new procedures. P1 and P3 felt the training was instrumental in overcoming the mindset barrier of several employees who found difficulty in overcoming the need to retain a paper copy. P1, P2, P3, P4, and P5 all felt the ongoing training of employees along with continual education of customers contributed to the smooth transition to the new policies and procedures. Additionally, all study participants spoke to the importance of strong support of the new policies and procedures by business owners and management stating this is integral to the success of the new strategies. All five study participants felt that continuing vigilance by owners and managers reflected the strong buy in to the new policies and aided in acceptance by employees and ensuring continuing compliance. Table 3 is a display of the tactics used by the participants to implement their training and education strategy.

Table 3

Tactics Used to Implement the Training and Education Strategies

Tactic	Percent of Use by Owners
Strong buy in and support of owners and management	100%
Extensive and ongoing training of employees	100%
Education of customers on new procedures	100%
Continual vigilance to ensure compliance	100%

P2 stated, "Visible and strong buy in of the new strategies by owners and management" was integral to the successful implementation of the new strategies and employee adherence to new procedures. P5 commented, "Without strong buy in by owners and managers, how can one expect employees to come on board with the new strategies." All five participants felt that strong buy in of the new strategies, policies, and procedures helped to convince employees of need and the importance to comply. P1 commented, "Strong buy in by owners and management along with a schedule of ongoing mandatory training" sent a very strong message to employees regarding the importance of the new strategies to the business. P1 further stated, "Initial and ongoing training of employees is key to the acceptance to and compliance with the new policies and procedures." P3 agreed with P1, stating, "Strong buy in along with extensive training helps employees to overcome any barriers to compliance they may harbor." P2 and P4 agreed that strong support of the new strategies by owners and managers provided a strong foundation for success for employees.

P4 stated, "Along with employee training, educating the customer to the new procedures was needed." P2 commented, "Educating the customer helps in the success of

the new strategies and also bolsters employee compliance." P5 stated, "Educating the customers to the new procedures helped generate trust and confidence in the business" and helped to overcome the barrier of employees' concerns that they would lose customers. Both P2 and P4 felt that when the customer is aware of the new procedures, they become additional eyes and ears of the owners and managers and aid in ensuring compliance with the new strategies. P2 and P4 further noted that customers are a great source of information about what is "being done right and what is being done wrong" in a business from the customer's point of view and can be a valuable source of information.

P3 stated, "To ensure employee compliance with the new strategies, owners and managers must be continually vigilant." P1 agreed stating, "Daily vigilance is necessary to ensure employee compliance and underscore the strong buy in to the new strategies by owners and managers." P1, P3, and P5 all acknowledged that they monitor employees daily, retain records of noncompliance, and deal with employees' noncompliance immediately.

I verified the interview data regarding training and education through a review of employee training manuals, educational flyers and posters designed to alert customers to the new procedures. The training manuals clearly detailed the new policies and procedures along with a brief explanation of the reasoning behind the changes. The flyers and posters designed for the customers provided some of the reasoning behind the changes. I also reviewed records that reflected the status of employee compliance with the new policies and procedures. P1, P3, and P5 tracked employee compliance daily with all instances of noncompliance fully documented and retained in their personnel file. P1

and P3 maintained a yearly calendar reflecting regular training classes available to all new and existing employees.

The findings regarding the implementation of training and education strategies align with the fraud triangle and fraud diamond theories because, as discussed by Cressey (1953) and Wolfe and Hermanson (2004), one of the most powerful tools available to owners and managers in the fight against the effects of fraud in business is training and education not only of owners and managers, but of employees and customers as well as all are a valuable part of the equation in fighting the effects of fraud. Through continual education and training, businesses are in a better position to mitigate the effects of identity theft and other frauds in their business.

The findings regarding education and training confirmed the research by Mangala and Kumari (2015) who pointed out that understanding the underlying causes of fraud leads to the implementation of strong fraud detection and mitigation strategies in reducing the effects of fraud on hospitality industry organizations of which the training and education of employees and customers is an integral part. Business leaders cannot rely solely on the information security system they have in place, but must also take into consideration the human equation (Kauspadiene et al., 2019). The findings regarding the importance of employee training and customer education confirmed the research by Kauspadiene et al. (2019). Security policies are formalized procedures and guidelines designed to safeguard sensitive information when used properly by employees (Cram et al., 2019). Without the proper training and education of employees, management support of the new policies, and constant vigilance to ensure compliance even the best

information security system will not be successful (Cram et al., 2019). The findings confirmed the research of Cram et al. (2019) who noted the importance of the partnership between training and vigilance to ensure compliance with the new strategies. Business owners, management, and employees may initially understand security policies and procedures differently highlighting the need for proper training of all involved to ensure the success of the new policies (Samonas, Dhillon, & Almusharraf, 2020). The findings confirmed the research by Samonas et al. (2020) regarding the need to ensure everyone involved in implementing the new strategies understand the new policies and procedures. All five participants felt continual training of employees and education of customers was extremely important when implementing the new information security procedures and policies and ensuring compliance by employees. This finding confirmed the research of Cram et al., Kauspadiene et al., and Samonas et al. who underscored the value of proper and ongoing training in addition to the information security system.

Theme 3: Vigilance Strategy

The third theme that emerged was the need for constant vigilance by business owners and upper management. P1, P2, P3, P4, and P5 all agreed that constant vigilance was the key to ensuring employee compliance and staying up-to-date and informed was an essential need to successfully mitigate the effects of identity theft. Table 4 is a display of the specific areas the participants felt were important in staying up-to-date and vigilant in mitigating the effects of identity theft in their business.

Table 4

Tactics Used to Implement Vigilance Strategies

Tactic	Percent of Use by Owners
Remaining aware of current and upcoming technologies	100
Update policies, procedures, and strategies as needed	100
Zero-tolerance policies	100
Continual training of employees	100
Continual education of customers	100

All five participants also mentioned the need for business leaders to stay informed of new technologies and strategies to mitigate identity theft. P1, P3, and P5 felt that staying current and updating policies, procedures, and strategies as needed was critical to protecting the business and its customers. P1 commented, “The best defense is a good offense through utilizing new technologies and strategies as they become available.” P3 echoed the sentiment of P1, stating, “For businesses to remain successful in the fight against fraud, staying informed with advances in technology is vital.” While various comments by P2 and P4 in general agreed with statements by the other participants, P2 and P4 felt other lower technology or no technology measures were more appropriate and just as successful for their businesses. Both P2 and P4 chose to go with an all cash strategy. P2 stated, “Going to an all cash strategy is easier for the employees.” P4 stated, “The all cash strategy is much more budget friendly and easier to implement.” All participants commented that identity theft is an ongoing challenge, especially for businesses with limited resources. Due to budgetary constraints, P2 and P4 chose to forgo

investing in new technology, but still implemented strict policies and procedures regarding retention of sensitive business and customer information.

P3 commented, “Staying up-to-date on available technologies and successful strategies to mitigate the effects of fraud in businesses was integral when updating policies, procedures, and strategies.” P1 and P5 both mentioned that ongoing research in mitigating loss due fraud helped them keep their policies, procedures, and strategies up-to-date. P2 and P4 also felt that keeping up on trends in technology and fighting fraud in businesses was important to alert them to needed changes in policies and strategies. All five participants agreed on the vital need for business owners to stay informed and be willing to update the technology and policies that are in place as needed. All participants acknowledged the importance of continual vigilance to mitigate the effects of identity theft.

One facet of continual vigilance is a zero-tolerance policy. A zero-tolerance policy means that leaders will not tolerate noncompliance with implemented policies and procedures and the violator will be subject to immediate termination (Samonas et al., 2020). Not only does a zero-tolerance policy reflect strong support by owners and management for the new strategies, the policy is a means for leaders to highlight the importance of the policies and procedures to the success of the business, and puts all employees on notice that they are being monitored for compliance. P3 stated, “Instances of noncompliance have been greatly reduced after the implementation of a zero-tolerance policy.” P5 stated, “There are rarely instances of noncompliance since the zero-tolerance policy was instituted.”

The other facet of continual vigilance is ongoing training of both employees and customers. P4 declared, “The initial training of employees, coupled with regular ongoing training on the policies and procedures aids in encouraging compliance.” P1 stated, “Ongoing training of employees and education of customers is instrumental in overcoming barriers to implementation and made the transition to electronic only records very smooth.” P2 stated, “Training employees along with educating customers ensured buy in by both parties while reflecting the strong backing by owners and management.” P4 commented that by training employees and educating customers, employees were more likely to comply because too many people knew the policies and were watching to make sure they followed the policies. All five participants felt training of employees along with educating customers was integral in the success of the policies and strategies implemented as it encouraged everyone to work together for success.

I verified the vigilance strategies through a review of company memos and notes, employee training manuals, policy and procedure manuals, and compliance policy documents. The memo and notes documented the research conducted to date into new technologies and successful fraud mitigation strategies, as well as recording the ongoing research by owners and managers to stay informed. The memos also referred to updates to the policies and strategies needed based on the participants’ research and how they implemented the changes.

The reviewed policy manuals from each business contained similar zero-tolerance wording, such as “Employees that do not comply with the policies and procedures contained therein will be subject to immediate termination.” P1, P3, and P5 included a

compliance policy document that contained a requirement for each employee to sign, date, and turn in as verification they understood the terms of the compliance policy. P1, P3, and P5 retained the signed compliance policy in the employee's personnel file. P2 and P4 did not require employees to sign a compliance policy document, but did post signs directed at employees to constantly remind them of the zero-tolerance policy and the ramifications if not complied with. All the documents reviewed sent a very strong message from upper management to employees.

The findings regarding the implementation of vigilance strategies align with the fraud triangle and fraud diamond theories because, as pointed out by Cressey (1953) and Wolfe and Hermanson (2004), business leaders need to be proactive in staying current not only on what frauds are being perpetrated that could affect their business, but also in what new and upcoming technologies and strategies are available to business leaders. Cressey as well as Wolfe and Hermanson stated that business owners need to understand motivation and opportunity to aid in developing policies that ensure employee compliance. In this regard, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity developed a framework comprised of five continuous functions for cybersecurity management strategy: identify, protect, detect, respond, and recover (Bjorke & May, 2016).

Although not committing fraud, if employees feel the opportunity to circumvent or completely ignore the new policies are present, they will likely not comply with the new policies (Free, 2015; Lokanan, 2018). Add motivation to opportunity and the employee is more likely to choose not to comply with the new policies (Ruankaew,

2016). While most employees will comply, there are those that may feel the new policies are an imposition or are too complicated and knowingly decide not to comply, thus violating the new policies (Cram et al., 2019; Moody, Siponen, & Pahnila, 2018). The findings confirmed the research by Cram et al. (2019), Lokanan (2018), and Moody et al. (2018) regarding the need for business owners to be vigilant to ensure compliance.

Although no one solution will work for every business, commonalities include the need for the continuous collection of cybersecurity risks and incidents, the development and implementation of effective cybersecurity policies, and the regular review of assessments, policies, budgets, response plans, and insurance with revisions made as needed (Bjorke & May, 2016). The finding of a vigilance strategy to mitigate the effects of identity theft and fraud in hospitality businesses confirmed the research of Alalehto (2018) who noted that hospitality leaders need to develop and continually update strategies that reduce or eliminate the elements of fraud within the constraints of their budget and available resources. The findings also confirm the research by Kauspadience et al. (2019) and Samonas et al. (2020) who underscored the importance for business leaders to stay current with new technologies and information security systems available within the budgetary restrictions and needs of the specific business.

Applications to Professional Practice

Fraud, including identity theft, continues to increase in the hospitality business (Abdullahi & Mansor, 2018; Bjorke & May, 2016). Business leaders in the hospitality industry are ultimately responsible for the detection and mitigation of the effects of identity theft in their businesses (Mangala & Kumari, 2015). All participants in this study

stressed the need for industry leaders to stay up-to-date on new and upcoming technologies and strategies to mitigate the cost of identity theft in their business, shared the strategies they tried, and shared in detail which strategies worked best for them and why. While larger businesses have the resources to utilize upscale sophisticated technologies, smaller businesses do not have these resources. One major common denominator of the successful strategies to mitigate the effects of identity theft in their business shared by all the participants was that they tailored the strategies to the specific business, were budget friendly, and within reach of small businesses with limited resources.

Business owner might apply the findings to implement new technology strategy. Internet commerce and the ease of doing business online requires consumers to release sensitive information, such as bank or credit card numbers, name and address, and other sensitive identifying information (Ashenmacher, 2016; DiSanto, 2015). Effective, affordable software and technology is available to businesses of all sizes (Ashenmacher, 2016). Some of the available technology includes chip-enabled credit card readers along with gathering identifying information from the customer, such as requiring picture identification for onsite transactions, and storing sensitive customer information in a secure electronic format to include offsite secure LAN servers (Carlino, 2018; Froud, 2015). Business owners can gain access to electronic storage by using Cloud storage along with very strict security access, thus protecting both the business' and customers' sensitive information from falling into the wrong hands.

Hospitality business owners could apply the findings to implement an education and training strategy to mitigate the effects of fraud and identity theft. In conjunction with secure information gathering and storage systems, all the participants noted that updated policies and procedures along with initial and ongoing employee training was another link in successfully mitigating the effects of identity theft in their businesses. The process includes educating the customer as well to new procedures designed to protect their information. Regular training of employees ensures they are aware of the policies and procedures as well as owner and management support of these policies and procedures. However, even the best system and strictest policies and procedures alone are not enough.

The strongest force in the struggle to mitigate the effects of identity theft in business is the employees, supervisors, and managers who are on the front lines every day dealing with each transaction. If business leaders cannot get everyone on board with the new strategies, even the best strategies will be useless. The study participants all agreed that strict compliance with the updated policies and procedures is essential to the success of the new strategies. To this end, the study participants have instituted a zero-tolerance policy and monitor compliance daily. If a manager, supervisor, or employee does not adhere to the policies and procedures, they are subject to immediate termination. This sends a strong message of support by owners and business leaders as to the importance of the new strategies.

Owners of hospitality businesses might apply the finding to implement a vigilance strategy. All study participants agreed that business owners and leaders must keep

informed and up-to-date regarding trends in identity theft and other frauds in the hospitality industry along with new and upcoming information security technology and successful strategies. Business owners and leaders must be willing to update strategies as needed to keep current with the constantly changing field of identity theft. The National Institute of Standards and Technology developed a list of five continuous functions for business leaders to employ in the fight against identity theft: identity, protect, detect, respond, and recover (Bjorke & May, 2016). Although, no one-size-fits-all answer exists to mitigate the effects of identity theft, there are several successful mitigation tools available to business leaders that fit all budgets.

Implications for Social Change

Business leaders in the hospitality industry may use the findings of this study to affect social change through ongoing detection of fraudulent transactions, increased safeguarding and the security of sensitive business and customer information, and reduced costs to both the business and the customer. The implications for social change include the possibility of small businesses to be successful; thereby employing more people and providing more services to more customers. Remaining successful in business contributes to a healthy and growing local economy.

The findings in this study are also in alignment with the recommended best practices by the federal government, including the Federal Trade Commission, National Institute of Standards and Technology, the National Association of Corporate Directors, and the Information Systems Audit and Control Association (Bjorke & May, 2016). These organizations recommended that businesses utilize strong information security

protocols, implementation of appropriate policies and procedures, ongoing mandatory training of employees, staying current on new technologies and successful strategies, and the willingness to adjust and update strategies, policies and procedures as needed (Bjorke & May, 2016). By following the recommendations in this study, both the businesses' and customers' sensitive information will be more secure generating more trust in the business from the customers which leads to more loyalty by customers thus increasing business revenues contributing to a healthier and more robust local economy.

Business leaders might use the three themes that emerged from this study to gain important and effective tools to aid in the success of their businesses. Implementing new technology strategies to keep sensitive business and customer information secure from fraud could result in trust and loyalty from customers. Implementing training and education strategies support the technology strategies for leaders to ensure employees follow the new strategies and customers understand the new policies, which could further customer trust and confidence in the business. Business leaders including ongoing vigilance strategies is a way to improve compliance by employees and help the leaders to stay on the forefront of new technologies and be successful in mitigating the effects of fraud. By utilizing all three fraud mitigation strategies in tandem, business owners might foster trust and loyalty from customers, which in turn is a means for the owners to aid in the success of the business generating additional employment opportunities and leading to a healthy economy.

Recommendations for Action

Identity theft negatively affects the profitability of businesses in the hospitality industry because some business leaders in the hospitality industry lack successful strategies to mitigate the effects of identity theft. The findings of this study indicated that business owners used new technologies, training and education, and vigilance strategies to successfully mitigate the effects of identity theft in their business. I recommend to business owners to utilize the latest in information security technology to secure both business and customer information. By implementing available information security technology, business owners will have the tools to effectively protect sensitive information from unauthorized individuals. Many information security systems companies offer secure access and off-site servers in addition to customizability, providing the business owner the ability to go paperless. There are information security technology systems available to fit any budget and most are customizable to the needs of each individual business (Bjorke & May, 2016).

I also recommend to business owners the need for comprehensive and ongoing training of employees along with educating customers of the policies in effect. Employees must know what the policies are and fully understand what employers expect of them. Regular training is a means for business owners to ensure everyone in the company understands the procedures required to effectively implement the policies. Additionally, by educating the customer on the policies there is less resistance from customers, making implementation of the policies much smoother. Consistent and

ongoing training is a strategy for leaders to remove barriers to successful implementation and ensure everyone in the organization understands the reasoning behind the policies.

To further ensure the success of the mitigation strategies, I also recommend business leaders institute an ongoing vigilance strategy. With a zero-tolerance policy, business owners can monitor and ensure compliance with the new mitigation strategies by employees. Zero-tolerance policies are a means for employers to show the employees there is strict buy in to the new strategies by owners and management, and the importance of compliance. Business leaders also need to stay current regarding new and upcoming information security technology and successful mitigation strategies through ongoing research. By remaining up-to-date regarding technology and strategy, business leaders will possess the ability to update their policies as new mitigation strategies become available.

By implementing these recommendations, business leaders will potentially have the tools needed to create an extremely effective, affordable, and customizable mitigation strategy, regardless of business size. I plan to disseminate the findings of this study by providing an executive summary of the results to all study participants. I will submit articles for publication in the *Fraud Magazine*, *The Tavern Times,* and various hospitality industry publications. I will seek opportunities to present the findings at one or more of the *Association of Certified Fraud Examiners'* many conferences and training sessions as well as local fraud conferences. I will also make my findings available to various state government agencies who have already expressed an interest in this study.

Recommendations for Further Research

This study was a qualitative case study limited to five leaders in the hospitality industry in the state of Montana. The limited scope of this study may restrict the transferability of the findings. The limitations of this study lead to several recommendations for further research. My first recommendation is that future researchers conduct multiple case studies to expand the population to other industries in Montana to compare possible differences in successful fraud mitigation strategies by industry. Conducting research in other industries would include increasing the number of study participants as well providing the future researcher with broader access to information and possibly, additional themes. My second recommendation is that future researchers conduct mixed-method studies to utilize the information gathered through a qualitative method to use in tandem with data collected through a quantitative method. The findings of a mixed-method study would be generalizable to larger populations, which would overcome a key weakness of my study. My third recommendation is that by expanding the study to all industries in a specific location, future researchers could compare the successful fraud mitigation strategies between large and small businesses, highlighting any differences related to business size or availability of resources.

Reflections

My choice in deciding to conduct a study on mitigating the effects of fraud in the hospitality business stemmed from my years working as a regulator in the hospitality business as well as being an owner of a small business in the hospitality business. The journey through the doctoral process was more rigorous that I initially expected, but also

more rewarding than I expected. For perhaps the first time in my scholastic journeys, I became challenged to expand my horizons and truly learn. There were a few surprises I was not expecting from working with study participants. I assumed business owners would be far more willing to participate, yet I had many people decline to be a participant. I overcame this hurdle by remaining dedicated and persistent, and was finally able to complete my interviews and data gathering. I was also surprised by the pervasiveness of the belief that there is no fraud in Montana. This doctoral journey has turned out to be one of the most challenging, yet rewarding experiences of my life. I learned a lot about myself and others. During the journey I found myself making notes for potential future studies that interested me. While I completed this journey, the next one looms on the horizon.

Conclusion

Leaders in the U.S. hospitality industry experience significant losses in profitability, increased mitigation cost, and reduced revenues because of identity theft. The purpose of this qualitative multiple case study was to explore the strategies leaders in the hospitality industry use to mitigate the effects of identity theft. The conceptual framework used in this study was a combination of the fraud triangle theory and the fraud diamond theory. A purposeful sample of five leaders of five different hospitality businesses in the state of Montana participated in the study. I collected data through semistructured interviews, member checking, and a review of company documents. During data analysis using Yin's five-step process, three key themes emerged: a new technology strategy, a training and educating strategy, and a vigilance strategy. The

findings indicated that leaders in the hospitality industry mitigate the effects of identity theft by implementing strategies to use up-to-date technology, train employees, educate consumers, and improve their vigilance. The implications for positive social change include the potential for leaders in the U.S. hospitality industry to increase consumer confidence, improve security for consumer data, and reduce consumer financial losses as a result of identity theft.

References

Abdalla, M. M., Oliveria, L. G., Azevedo, C. E. F., & Gonzalez, R. K. (2017). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administracao: Ensino E Pesquisa, 19*(1), 66-98. doi:10.13058/raep.2018.v19n1.578

Abdullahi, R., & Mansor, N. (2018). Fraud prevention initiatives in the Nigerian public sector: Understanding the relationship of fraud incidences and the elements of fraud triangle theory. *Journal of Financial Crime, 25*, 527-544. doi:10.1108/JFC-02-2015-0008

Adams, C., & van Manen, M. A. (2017). Teaching phenomenological research and writing. *Qualitative Health Research, 27*, 780-791. doi:10.1177/1049732317698960

Adashi, E. Y., Walters, L. B., & Menikoff, J. A. (2018). The Belmont Report at 40: Reckoning with time. *American Journal of Public Health, 108*, 1345-1348. doi:10.2105/AJPH.2018.304580

Alalehto, T. (2018). Crime prevention in terms of criminal intent criteria in white collar crime: A propositional analysis. *Journal of Financial Crime, 25*, 838-844. doi:10.1108/JFC-05-2017-0051

Albrecht, S., Howe, K., & Romney, M. (1984). Deterring fraud: The internal auditor's perspective. *Institute of Internal Auditors Research Foundation,* 1-42. Retrieved from https://www.isaca.org

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity, 23,* 121-127. Retrieved from www.ncbi.nlm.nih.gov/journals/j-cult-drivers/

Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: framework for the retail industry. *International Journal of Retail and Distribution Management, 46*(4), 350-363. doi:10.1108/IJRDM-10-2016-0185

Amato, N. (2016, July 25). The hidden costs of a data breach. *Journal of Accountancy*. Retrieved from www.journalofaccountancy.com/news/2016/jul/

Antonescu, M., & Birau, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance, 32,* 618-621. doi:10.1016/S2212-5671(15)01440-9

Ashenmacher, G. (2016). Indignity: Redefining the harm caused by data breaches. *Wake Forest Law Review, 51,* 1-56. Retrieved from www.wakeforestlawreview.com

Association of Certified Fraud Examiners. (2018). *Report to the nations: 2018 Global study on occupational fraud and abuse.* Austin, Texas: Author

Azam, M. R. (2018). Theory application: Why people commit fraud. *International Journal of Management, Accounting and Economics, 5*(1), 54-65. Retrieved from www.ijmae.com

Baesens, B., Vlasselaer, V., & Verbeke, W. (2015). *Fraud analytics using descriptive and social network techniques.* Charlotte, NC: Wiley and SAS Business Series.

Baillie, L. (2015). Promoting and evaluating scientific rigour in qualitative research. *Nursing Standard, 29*(46), 36-42. doi:10.7748/ns.29.46.36.e8830

Baker, C. R., Cohainer, B., & Leo, N. J. (2016). Considerations beyond the fraud triangle in the fraud at Societe General. *Journal of Forensic & Investigative Accounting, 8*(3), 462-479. Retrieved from www.nacva.com

Baker, J. D. (2016). The purpose, process, and methods of writing a literature review. *AORN Journal, 103,* 265-269. doi:10.1016/j.aorn.2016.01.01

Banarescu, A. (2015). Detecting and preventing fraud with data analytics. *Procedia Economics and Finance, 32,* 1827-1836. doi:10.1016/S2212-5671(15)01485-9

Barnham, C. (2016). Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research, 57,* 837-854. doi:10.2501/ijmr-2015-007

Basta, Y. L., Tytgat, K. M. A. J., Klinkenbijl, J. H. G., Fockens, P., & Smets, E. M. A. (2016). Waiting time at a fast-track diagnostic clinic. *International Journal of Health Care Quality Assurance, 29,* 523-535. doi:10.1108/IJHCQA-09-2015-0116

Becker, L. (2018). Methodological proposals for the study of consumer experience. *Qualitative Market Research, 21,* 465-490. doi:10.1108/QMR-01-2017-0036

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in Qualitative research. *Qualitative Research, 15*, 219-234. doi:10.1177/1468794112468475

Bernard, H. R., Wutich, A., & Ryan, G. W. (2016). *Analyzing qualitative data: Systematic approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Birchall, J. (2014). Qualitative inquiry as a method to extract personal narratives: Approach to research into organizational climate change mitigation. *The Qualitative Report, 19*(75), 1-18. Retrieved from https://nsuworks.nova.edu/tqr/

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26,* 1802-1811. doi:10.1177/1049732316654870

Bjorke, J., & May, D. (2016). Trends in recent data breach litigation. *Franklin Business and Law Journal, 2016*(4), 52-66. Retrieved from www.franklinpublishing.net

Blackwood, R. A., Maio, R. F., Mrdhenovich, A. J., VandenBosch, T. M., Gordon, P. S., Shipman, E. L., & Hamilton, T. A. (2015). Analysis of the nature of IRB contingencies required for informed consent document approval. *Accountability in Research: Policies & Quality Assurance, 22,* 237-245. doi:10.1080/08989621.2014.956866

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research 19,* 426-432. doi:10.1108/QMR-06-2016-0053

Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud models use on auditor's fraud risk judgements. *Journal of Accounting and Public Policy, 34,* 578-596. doi:10.1016/j.jaccpubpol.2015.05.006

Burke, D. D., & Sanney, K. J. (2018). Applying the fraud triangle to higher education: Ethical implications. *Journal of Legal Studies Education, 35*(1), 5-43. Retrieved from www.journals.uchicago.edu

Carlino, N. (2018). How hotels can mitigate their fraud risk. *Hotel Business, 27*(10), 14. Retrieved from www.hotelbusiness.com

Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining based system for credit-card fraud detection in e-tail. *Decision Support Systems, 95*, 91-101. doi:10.1016/j.dss.2017.01.002

Cascio, M. A., & Racine, E. (2018). Person-oriented research ethics: Integrating relational and everyday ethics in research. *Accountability in Research, 25*, 170-197. doi:10.1080/08989621.2018.1442218

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21,* 811-831. Retrieved from https://nsuworks.nova.edu.tqr/

Cavalcanti, M. F. R. (2017). Guidelines for qualitative research in organization studies: Controversy and possibilities. *Administracao: Ensino E Perquisa, 18,* 457-488. doi:10.13058/raep.2017.v18n3.522

Cheraghalizadeh, R., & Tumer, M. (2017). The effect of applied resources on competitive advantage in hotels: Mediation and moderation analysis. *Journal of Hospitality and Tourism Management, 31*, 265-272. doi:10.1016/j.jhtm.2017.04.001

Chong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *American Journal of Management, 11*(1), 59-68. Retrieved from http://www.na-businesspress.com/ajmpen.html

Clark, K. R., & Veale, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89*, 482CT-485CT. Retrieved from www.radiologictechnology.org

Cohn, M. (2015). IRS beefing up detection of business identity theft. *Accounting Today, November 2015.* Retrieved from www.accountingtoday.com

Coleman, J. S. (1990). *Foundations of social theory.* Cambridge, MA: Harvard University Press.

Compin, F. (2016). Do financial criminals commit perfect crimes? *Journal of Financial Crime, 23,* 624-636. doi:10.1108/JFC-03/2015/0018

Connelly, L. M. (2016). Trustworthiness in qualitative research. *MEDSURG Nursing, 25*, 435-436. Retrieved from www.medsurgnursing.net

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*(1), 89-91. doi:10.1188/14.ONF.89-91

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019) Seeing the forest for the trees: A meta-analysis of the antecedents of information security policy compliance. *MIS Quarterly, 43*, 525-554. doi:10.25300/MISQ/2019/15117

Cressey, D. R. (1953). *Other people's money: The social psychology of embezzlement*. New York, NY: The Free Press.

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing, 36,*253-263. doi:10.1097/DCC.0000000000000253

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE transactions on Neural Networks and Learning Systems, 29*, 3784-3797. doi:10.1109/TNNLS.2017.2736643

Dasgupta, M. (2015) Exploring the relevance of case study research. *Vision, 19*(2), 147-160. doi:10.1177/0972262915575661

Davidson, J., Thompson, S., & Harris, A. (2017). Qualitative data analysis software practices in complex research teams: Troubling the assumptions about transparency and portability. *Qualitative Inquiry, 23,* 779-788. doi:10.1177/1077800417731082

De Bock, T., & Van Kenhove, P. (2011). Double standards: The role of techniques of neutralization. *Journal of Business Ethics, 99*, 283-296. doi:10.1007/s10551-010-0654-3

DiSanto, P. F. (2015). Blurred lines of identity crimes: Intersection of the first amendment and federal identity fraud. *Columbia Law Review, 115,* 941-982. Retrieved from www.columbialawreview.org

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education, 27*, 555-579. doi:10.2308/iace-50131

Downing, C. O., Capriola, N., & Geller, E. S. (2018). Preventing credit card fraud: A goal setting and prompting intervention to increase cashiers' ID checking

behavior. *Journal of Organizational Behavior Management, 38*(4), 335-344. doi:10.1080/01608061.2018.1514349

Drouin, M., Stewart, J., & Van Gorder, K. (2015). Using methodological triangulation to examine the effectiveness of a mentoring program for online instructors. *Distance Education, 36,* 400-418. doi:10.1080/01587919.2015.1081735

Eisenberg, P. (2017). Financial crime – is there any way out of the theoretical deadlock? *Journal of Financial Crime, 24*, 529-540. doi:10.1108/JFC-06-2016-0043

Ernst & Young, LLP. (2016). *Managing fraud, bribery and corruption risks in the hospitality industry.* Retrieved from www.ey.com

Federal Reserve Bank. (2019). *Synthetic identity fraud in the U.S. payment system.* Washington D.C.: Author.

Federal Trade Commission. (2018). *Consumer Sentinel Network Data Book 2017*. Retrieved from www.ftc.gov

Felson, M. (2008). Routine activity approach. In R. Wortley & L. (Eds), *Environmental criminology and crime analysis.* New York, NY: Willan Publishing.

Firmin, R. L., Bonfils, K. A., Luther, L., Minor, K. S., & Salyers, M. P. (2017). Using text-analysis computer software and thematic analysis on the same qualitative data: A case example. *Qualitative Psychology, 4*, 201-210. doi:10.1037/qup0000050

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security. 61,* 169-183. doi:10.1016/j.cose.2016.06.002

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

Free, C., Macintosh, N., & Stein, M. (2007). Management controls: The organizational fraud triangle of leadership, culture and control in Enron. *Ivey Business Journal, 17,* 1-8. Retrieved from https://iveybusinessjournal.com/

French, J. R. P., & Raven, B. (1959). *The bases of social power: Group dynamics.* New York: Harper & Row.

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont Report? *The American Journal of Bioethics, 17*(7), 15-21. doi:10.1080/15265161.2017.1329482

Froud, D. (2015). The central role of authentication in fighting fraud in mobile commerce. *Journal of Payments Strategy & Systems, 9*(4), 274-279. Retrieved from www.henrystewartpublications.com/jpss

Furlan, S., & Bajec, M. (2008). Holistic approach to fraud management in health insurance. *Journal of Information and Organizational Sciences, 32*(2), 99-114. Retrieved from http://journal-iostudies.org/

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20,* 1408-1416. Retrieved from https://nsuworks.nova.edu/tqr/

Garcia, A. O. (2018). *Strategies to reduce occupational fraud in small restaurants* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Database. (UMI No. 10812913)

Genel, A., & Topcu, M. S. (2016). Turkish preservice science teachers' socioscientific issues-based teaching practices in middle school science classrooms. *Research in Science & Technology Education, 34*(1), 105-123. doi:10.1080/02635143.2015.1124847

Global Hospitality Portal. (2018). *What are the 5 different sectors of hospitality industry?* Retrieved from https://www.soegjobs.com/2016/09/07/different-sectors-hospitality-industry/

Gog, M. (2015). Case study research. *International Journal of Sales, Retailing & Marketing, 4*(9), 33-41. Retrieved from http://www.ijsrm.com/

Golladay, K. A. (2017). Reporting behaviors of identity theft victims: An empirical test of Black's theory of law. *Journal of Financial Crime, 24*(1), 101-117. doi:10.1108/jfc-01-2016-0010

Gottschalk, P. (2010). Theories of financial crime. *Journal of Financial Crime, 17*, 210-222. doi:10.1108/13590791011033908

Grady, C. (2015). Enduring and emerging challenges of informed consent. *New England Journal of Medicine, 372,* 855-862. doi:10.1056/NEJMra1411250

Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Newbury Park, CA: Sage.

Guetterman, T. C., & Fetters, M. D. (2018). Two methodological approaches to the integration of mixed methods and case study designs: A systematic review. *American Behavioral Scientist, 62*, 900-918. doi:10.1177/0002764218772641

Harrell, E. (2015). Victims of identity theft. *Bureau of Justice Statistics, September 2015,* 1-25. Retrieved from https://www.bjs.gov/content/pub/pdf/vit14.pdf

Helena Chamber of Commerce. (2018). Retrieved from https://helenachamber.com

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: How many interviews are enough? *Qualitative Health Research, 27,* 591-608. doi:10.1177/1049732316665344

Henson, A., & Jeffrey, C. (2016). Turning a clinical question into nursing research: The benefits of a pilot study. *Renal Society of Australasia Journal, 12,* 99-105. Retrieved from http://www.renalsociety.org/journal/

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30,* 1-19. doi:10.1016/j.intmar.2014.10.001

Horga, G., Kaur, T., & Peterson, B. (2014). Annual research review: Current limitations and future directions of MRI studies of child and adult onset development sychopathologies. *Journal of Child Psychology and Psychiatry, 55*, 659-680. doi:10.1111/jcpp.12185

Huber, W. D. (2017). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research, 12*(2), 28-49. Retrieved from www.jtar.org

Hull, S. C., & Wilson, D. R. (2017). Beyond Belmont: Ensuring respect for AI/AN communities through tribal IRBs, laws, and policies. *American Journal of Bioethics, 17*(7), 60-62. doi:10.1080/15265161.2017.1328531

Hutagalung, I. (2016). Selective exposure and consumer behavior – interpretative phenomenological analysis in consumer behavior of Z generation adolescent on the ad information of smartphone selection. *International Journal of Organizational Innovation, 9*(2), 97-104. Retrieved from https://www.ijoi-online.org

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *International Journal of Computer Science and Network Security, 18*(1), 43-55. Retrieved from www.ijcsns.org

ITRC Annual Report. (2018). 2018 Annual Report – Identity Theft Resource Center. Retrieved from www.idtheftcenter.org

Iwejor, I. C. (2017). *Internal controls: Identifying control elements and implementation dynamics facing retail companies* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Publishing. (UMI No. 10690943)

Jervis, M. G., & Drake, M. A. (2014). The use of qualitative research methods in quantitative science: A review. *Journal of Sensory Studies, 29*, 231-247. doi:10.1111/joss.12101

Johnson, T. P. (2015). *Handbook of health survey methods*. Hoboken, NJ: John Wiley & Sons.

Joslin, R., & Muller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Program Management, 34,* 1043-1056. doi:10.1016/ijproman.2016.05.005

Kahn, C. M., & Linares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research, 50*(1), 121-159. doi:10.1007/s10693-015-0218-x

Kaplan, B. (2016). Evaluation of people, social, and organizational issues – sociotechnical ethnographic evaluation. *Studies in Health Technology & Informatics,* 222, 114-125. doi:10.3233/978-1-61499-635-4-114

Kauspadiene, L., Ramanauskaite, S., & Cenys, A. (2019) Information security management framework suitability estimation for small and medium enterprise. *Technology & Economic Development of Economy, 25*, 979-997. doi:10.3846/tede.2019.10298

Kilinc, H., & Firat, M. (2017). Opinions of expert academicians on online data collection and voluntary participation in social sciences research. *Educational Sciences: Theory & Practice, 17,* 1461-1486. doi:10.12738/estp.2017.5.0261

Kim, E. J., & Kim, S. H. (2015). Simplification improves understanding of informed consent information in clinical trials regardless of health literacy level. *Clinical Trials, 12,* 232-236. doi:10.1177/1740774515571139

Kohler, T. (2016). From the editors: On writing up qualitative research in management learning and education. *Academy of Management Learning & Education, 15,* 400-418. doi:10.5465/amle.2016.0275

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology, 12*, 397-414. doi:10.1080/14780887.2015.1021941

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

Kultur, Y., & Caglayan, M. U. (2017). Hybrid approaches for detecting credit card fraud. *Expert Systems, 34*(2), 1-13. doi:10.1111/exsy.12191

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson.

Liao, H., & Hitchcock, J. (2018) Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation and Program Planning, 68,* 157-165. doi:10.1016/j.evalprogplan.2018.03.005

Lokanan, M. E. (2015). Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum, 39*(2015), 201-224. doi:10.1016.j.accfor.2015.05.002

Lokanan, M. E. (2018). Informing the fraud triangle: Insights from differential association theory. *Journal of Theoretical Accounting Research, 14*(1), 55-98. Retrieved from www.jtar.org

Loker, M. (2018). Conveniently exposed: How the convenience of the internet is exposing you to identity theft. *Journal of Internet Law, 22*(2), 3-7. Retrieved from https://commlawgroup.com/product/journal-of-internet-law/

Mackevicius, J., & Giriunas, L. (2013). Transformational research of the fraud triangle. *Ekonomika, 92*(4), 150-163. doi:10.15388/ekon.2013.0.2336

Makrakis, V., & Kostoulas-Makrakis, N. (2016). Bridging the qualitative-quantitative divide: Experiences from conducting a mixed methods evaluation in the RUCAS programme. *Evaluation and Program Planning, 54*(1), 144-151. doi:10.1016/j.evalprogplan.2015.07.008

Mangala, D., & Kumari, P. (2015). Corporate fraud prevention and detection: Revisiting the literature. *Journal of Commerce and Accounting Research, 4*(1), 52-62. Retrieved from www.publishingindia.com

Maria, E., & Gudono, E. (2017). Empirical test of fraud triangle theory on local government (evidence from Indonesia). *International Journal of Applied Business and Economic Research, 15*(4), 233-248. Retrieved from http://www.iceeia.org/index.aspx

Marks, J. (2009). *Playing offense in a high-risk environment.* New York, NY: Crowe Horwath.

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Marti, J. (2016). Measuring in action research: Four ways of integrating quantitative methods in participatory dynamics. *Action Research, 14*(2), 168-183. doi:10.1177/1476750315590883

McLevey, J. (2015). Understanding policy research in liminal spaces: Think tank responses to diverging principles of legitimacy. *Social Studies of Science, 45,* 205-293. doi:10.1177/0306312715575054

McMahon, R., Pence, D., Bressler, L., & Bressler, M. S. (2016). New tactics in fighting financial crimes: Moving beyond the fraud triangle. *Journal of Legal, Ethical and Regulatory Issues, 19*(1), 16-25. Retrieved from www.scimagojr.com

Mellado, D., & Rosado, G. D. (2012). An overview of current information systems security challenges and innovations. *Journal of Universal Computer Science, 18*, 1598-1607. Retrieved from http://www.jucs.org

Meyer, C., Scarinici, N., Ryan, B., & Hickson, L. (2015). This is a partnership between all of us: Audiologists' perceptions of family member involvement in hearing rehabilitation. *American Journal of Audiology, 24*, 536-548. doi:10.1044/2015_AJA-15-2006

Miracle, V. A. (2016). The Belmont report: The triple crown of research ethics. *Dimensions of Critical Care Nursing, 35*, 223-228. doi:10.1097/dcc.0000000000000186

Montana Department of Justice – Gambling Control Division. (2018). Retrieved from https://dojmt.gov/gaming/

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-311. doi:10.25300/MISQ/2018/13853

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*, 1212-1222. doi:10.1177/1049732315588501

Muhtar, S., Sutaryo, M., & Sriyanto, S. (2018). Corruption in Indonesian local government: Study on triangle fraud theory. *International Journal of Business and Society, 19*, 536-552. Retrieved from http://www.ijbs.unimas.my/

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. doi:10.1108/ARJ-10-2014-0092

Murphy, P. R., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. *Behavioral Research in Accounting, 28*(1), 41-56. doi:10.2308/bria-51083

Murtha, L. F., & Lipkin, S. J. (2017). Ethical and operational issues related to clinical trial billing: What do HRPPs and IRBs need to consider? *Journal of Health Care Compliance, 19,* 23-30. Retrieved from http://www.healthcarecompliance.us

Nagasaka, K., Bocher, M., & Krott, M. (2016). Are forest researchers only scientists? Case studies on the roles of researchers in Japanese and Swedish forest policy processes. *Forest Policy and Economics, 70*, 147-154. doi:10.1016/.forpol.2016.06.006

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (NCPHSBBR). (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* Washington, DC: U.S. Department of Health and Human Services. Retrieved from hhs.gov/ohrp/humansubjects/guidance/Belmont.html

Nelson, A., & Cohn, S. (2015). Data collection methods for evaluating museum programs and exhibitions. *Journal of Museum Education, 40*(1), 27-36. doi:10.1080/10598650.2015.11510830

Norfara, N., Koo, P. M., & Siti-Nabiha, A. K. (2018). Private label brand purchase intention: A Malaysian study. *Global Business and Management Research, 10*(1), 197-215. Retrieved from www.gbmrjournal.com

Oliveria, M., Bitencourt, C. C., dos Santos, A. C. M. Z., & Teixeira, E. K. (2016). Thematic content analysis: Is there a difference between the support provided by the MAXQDA and NVivo software packages? *Brazilian Journal of Management, 9*(1), 72-82. doi:10.5902/1983465911213

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,* 1012-1027. doi:10.1108/JFC-04-2015-0020

Paulus, T. M., & Bennett, A. M. (2017). I have a love-hate relationship with ATLAS.ti: Integrating qualitative data analysis software into a graduate research methods course. *International Journal of Research & Method in Education, 40*(1), 19-35. doi:10.1080/1743727X.2015.1056137

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. *Nurse Researcher, 22*(4), 6-7. doi:10.7748/nr.22.4.6.s2

Raghaven, K., Desai, M. S., & Rajkumar, P. V. (2017). Managing cybersecurity and e-commerce risks in small businesses. *Journal of Management Science and Business Intelligence, 2*(1), 9-15. doi:10.5281/zenodo.581691

Ranjan, S., Maurya, M., Malviya, A., Yadav, R., Gupta, R., Mishra, M., & Rai, S. (2012). Building an information security infrastructure: A comprehensive framework towards a robust, resilient, and dependable infrastructure. *International Journal of Computer Science Issues, 9*, 414-419. Retrieved from http://ijcsi.org

Raval, V. (2018). A disposition-based fraud model: Theoretical integration and research agenda. *Journal of Business Ethics, 150*, 741-763. doi:10.1007/s10551-016-3199-2

Reeves, R. B. (2017). Inter-cultural mentoring for newcomer immigrants: Mentor perspectives and better practices. *International Journal of Evidence Based Coaching & Mentoring, 15*(1), 186-207. doi:10.24384/IJEBCM/15/1

Richardson, B., & Waldron, D. (2019). Fighting back against synthetic identity theft. *McKinsey & Company, 7*, 1-6. Retrieved from www.mckinsey.com

Roden, D. M., Cox, S. R., & Joung-Yeon, K. (2016). The fraud triangle as a predictor of corporate fraud. *Academy of Accounting and Financial Studies Journal, 20*(1), 80-92. Retrieved from www.scimagojr.com

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135. doi:10.1093/cybsec/

Ruankaew, T. (2016). Beyond the fraud diamond. *International Journal of Business and Economic Research, 7*(1), 474-476. Retrieved from http://www.ijbmer.com

Saber, J. A. (2016). *Determining small business cybersecurity strategies to prevent data breaches* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses Database. (UMI No. 10181342)

Samonas, S., Dhillon, G., & Almusharraf, A. (2020) Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management, 50,* 144-154. doi:10.1016/j.ijinfomgt.2019.04.011

Saunders, M. N. K., & Townsend, K. (2016). Reporting and justifying the number of Interview participants in organization and workplace research. *British Journal of Management, 27,* 836-852. doi:10.1111/1467-8551.12182

Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal, 29*(2), 107-121. doi:10.1057/sj.2013.1

Sen, R., & Borle, S. (2015). Estimating the context risk of data breach: An empirical approach. *Journal of Management Information Systems, 32,* 314-341. doi:10.1080/07421222.2015.1063315

Sherchand, J. B. (2017). Mission of institutional review board/ethical review committee. *Journal of Institute of Medicine, 39*(1), 1-2. Retrieved from http://www.jiom.com

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology, 21*, 619-634. doi:10.1080/13645579.2018.1454643

Small, W., Maher, L., & Kerr, T. (2014). Institutional ethical review and ethnographic research involving injection drug users: A case study. *Social Science & Medicine, 104*, 157-162. doi:10.1016/j.socscimed.2013.12.010

Snodgrass, J. G., Dengah, H. J. F., Lacy, M. G., Bagwell, A., Van Oostenburg, M., & Lende, D. (2017). Online gaming involvement and its positive and negative consequences: A cognitive anthropological "cultural consensus" approach to psychiatric measurement and assessment. *Computers in Human Behavior, 66*, 291-302. doi:10.1016/j.chb.2016.09.025

Song, Z. (2017). The debate between empirical and broader phenomenological approaches to research. *Tourism Management, 58*, 304-311. doi:10.1016/j.tourman.2016.03.016

Sow, A. N., Basiruddin, R., Mohammad, J., & Rasid, S. Z. A. (2018). Fraud prevention in Malaysian small and medium enterprises (SMEs). *Journal of Financial Crime, 25*, 499-517. doi:10.1108/JFC.05.2017.0049

Statewide Publishing-MT. (2018). *Capital regional telephone directory.* Retrieved from https://www.statewideYP.com

Tarin, E. (2017). Qualitative research and clinical methods. *Annals of King Edward Medical University, 23*(1), 5-6. doi:10.21649/akemu.v23il.1514

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). *Introduction to qualitative research methods: A guidebook and resource* (4th ed.) New York, NY: John Wiley & Sons.

Thorne, B. M., & Stryker, J. P. (2018). The “Dirty Dozen” tax scams plus 1. *Shippensburg University, ABD Journal, 7*(1), 1-22. Retrieved from https://www.ship.edu/ABDjournal/Publications/

Tibben, W. J. (2015). Theory building for ICT4D: Systemizing case study research using theory triangulation. *Information Technology for Development, 21,* 628-652. doi:10.1080/02681102.2014.910935

Tran, V., Porcher, R., Tran, V., & Ravaud, P. (2017). Predicting data saturation in qualitative surveys with mathematical models from ecological research. *Journal of Clinical Epidemiology, 82*, 71-78. doi:10.1016/j.jclinepi.2016.10.001

Tumele, S. (2015). Case study research. *International Journal of Sales, Retailing and Marketing, 4*(9), 68-78. Retrieved from https://ijsrm.com/IJSRM/Home.html

Turner, P., Kane, R., & Jackson, C. (2015). Combining methods to research an emergency department: A case study. *British Journal of Healthcare Management, 21*(2), 81-85. doi:10.12968/bjhc.2015.21.2.81

Unkovic, C., Sen, M., & Quinn, K. M. (2016). Does encouragement matter in improving gender imbalances in technical fields? Evidence from a randomized controlled trial. *PLoS One, 11,* 55-86. doi:10.1371/journal.pone.0151714

U.S. Department of Justice. (2016). *Financial fraud and identity theft.* Retrieved from https://www.justice.gov/usao-md/financial-fraud-and-identity-theft

Valerio, M. A., Rodriguez, N., Winkler, P., Lopez, J., Dennison, M., Liang, Y., & Turner, B. J. (2016). Comparing two sampling methods to engage hard-to-reach

communities in research priority setting. *BMC Medical Research Methodology, 16,* 1-12. doi:10.1186/s12874-016-0242-z

Vass, C., Rigby, D., & Payne, K. (2017). The role of qualitative research methods in discrete choice experiments: A systematic review and survey of authors. *Medical Decision Making, 37,* 298-313. doi:10.1177/0272989X16683934

Vohra, V. (2014). Using the multiple case study design to decipher contextual leadership behaviors in Indian organizations. *The Electronic Journal of Business Research Methods, 12*(1), 54-65. Retrieved from www.ejbrm.com

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. *Journal of Financial Crime, 26*(1), 372-381. doi:10.1108/JFC12-2017-0128

Weiss, S. H. (2017). *Internal controls possessed by small business owners* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses Database. (UMI No. 10742825)

Welch, C., & Piekkari, R. (2017). How should we (not) judge the 'quality' of qualitative research? A reassessment of current evaluative criteria in international business. *Journal of World Business, 52,* 714-725. doi:10.1016/j.jwb.2017.05.007

Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of Economic Crime Management, 2*(2), 1-38. Retrieved from jecm.org

Wilson, V. (2016). Research methods: Triangulation. *Evidence Based Library and Information Practice, 11*(1), 66-68. doi:10.18438/b86s5f

Wolfe, D., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal, 74*(12), 38-42. Retrieved from https://www.cpajournal.com/

Wood, T., & da Costa, A. P. P. (2015). Corporate frauds as criminal business models: An exploratory study. *Thunderbird International Business Review, 57*(1), 51-62. doi:10.1002/tie.21676

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology, 88*, 225-231. Retrieved from http://www.radiologictechnology.org

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage Publications

Zaeem, R. N., Manoharan, M., Yang, Y., & Barber, K. S. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security, 65*, 50-63. doi:10.1016/j.cose.2016.11.002

Zainal, R., Som, A. M., & Mohamed, N. (2017). A review on computer technology applications in fraud detection and prevention. *Management & Accounting Review, 16*(2), 59-72. Retrieved from https://mar.uitm.edu.my

Appendix A: Interview Protocol

I will interview one leader from a bar, casino, restaurant, hotel/motel, and movie theater each of whom have been successful in mitigating fraud in their business. I will be conducting in-person interviews using semistructured open-ended questions using the following protocol:

1. I will introduce myself and explain that I am a doctoral student at Walden University. I will explain the purpose of my study and the interview.
2. Each participant will be provided a copy of the consent form prior to the interview. Once signed, I will thank the participant for agreeing to be part of the study.
3. I will explain and assure the participant that I will not reveal any personally identifiable information in the study and that all data will be destroyed after 5 years to maintain confidentiality.
4. I will inform each participant that the interview will be recorded with the interview lasting approximately 1 hour.
5. An opportunity for questions will be provided prior to beginning the interview.
6. The recorder will then be turned on and the interview will commence.
7. All study participants will be asked the same questions in the same order (see Appendix B).
8. During the interview, the participant's non-verbal cues will be observed, such as tone of voice, behavior, and gestures.
9. Reflective notes will be taken during the interview process.

10. When all questions have been asked and response provided, I will conclude the interview and stop the recording.
11. I will then explain the member checking process in which I will contact the participant within 15 business days with my interpretation of the data collected. At that time, the participant will have the opportunity to validate the accuracy of the information. I will allow the participant 10 days to review and confirm the findings or make any changes necessary.
12. I will provide the participant with my contact information for any possible questions or concerns.
13. I will again thank the participant for participating in the study.

Appendix B: Interview Questions

1. What strategies did you use to mitigate the effects of identity theft?
2. What strategies did you find to be most effective in mitigating the effects of identity theft for your business?
3. How did you assess the effectiveness of the strategies you implemented to mitigate identity theft?
4. What, if any, changes to your past process and procedures occurred to allow you to implement effective strategies to mitigate the effects of identity theft?
5. What barriers did you experience in implementing strategies to mitigate the effects of identity theft?
6. How did you overcome the barriers in implementing strategies to mitigate the effects of identity theft?
7. What other information would you like to add about the strategies used to mitigate identity theft in your business?