2022

Strategies Business Leaders Use to Mitigate Online Credit Card Fraud

Clarissa Rosario-Tavarez
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Clarissa Rosario-Tavarez

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. Elisabeth Musil, Committee Chairperson, Doctor of Business Administration Faculty

Dr. John Hannon, Committee Member, Doctor of Business Administration Faculty

Dr. Franz Gottleib, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2022

Abstract

Strategies Business Leaders Use to Mitigate Online Credit Card Fraud

by

Clarissa Rosario-Tavarez

MBA, Walden University, 2015

BS, Capital University, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2022

Abstract

Online credit card fraud targeting banks, customers, and businesses costs millions of U.S. dollars annually. Online business leaders face challenges securing and regulating the online payment processing environment. Grounded in the situational crime prevention theory, the purpose of this qualitative multiple case study was to explore strategies online business leaders use to mitigate the loss of revenue caused by online credit card fraud. The participants comprised five online business leaders of an organization in the Southwest of the United States, who implemented strategies that successfully mitigated revenue losses due to online credit card fraud. The data were collected from semistructured interviews, archival records, and business investment rating reports. Data were analyzed using Yin's five-step data analysis process. The following themes emerged from the data analysis: data management, analysis, and monitoring; internal stakeholders; customer experience; and partnership with online security tool service provider(s). Key recommendations to online business leaders include the development of system security strategies that ensure cardholders' and business' data protection, collaboration across departments in the organization to support fraud solutions, and customer engagement. The implications for positive social change include the potential to gain or retain consumer confidence in e-commerce and reduce consumers' collateral damage from credit card fraud.

Strategies Business Leaders Use to Mitigate Online Credit Card Fraud

by

Clarissa Rosario-Tavarez

MBA, Walden University, 2015

BS, Capital University, 2009

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2022

Dedication

I am profoundly and forever grateful to the Divine for showering me with grace, love, and strength to complete this rigorous but enriching program. I dedicate this dissertation to my beloved paternal grandparents Celestino Minaya (RIP) and Maria Severino de Minaya (RIP), my maternal grandparents, Andres Tavarez Pineda (RIP) and Natividad Reyes Lantigua, for their vision of possibilities for me and confidence in me to strive to achieve my goals. I also dedicate this dissertation to my parents, Carmen I. Tavarez Reyes and Carlos A. Rosario Minaya, for their encouragement and support. In addition, I dedicate this dissertation to my sons Armondy E. Nieves-Rosario and Axairus E. Nieves- Rosario, my most prominent supporters and my inspiration to complete this journey. Thank you, Axairus and Armondy, for your love, sacrifice, support, and reassurance. This achievement links my family's past, present, future.

Acknowledgments

I appreciate those who assisted me and encouraged me through this complex and transformational program. The completion of the DBA journey resulted from my arduous work, tenacity, and the guidance of Walden University's staff. I value the encouragement and support of my family and friends during this enriching program. Thank you, primarily to my chair committee, Dr. Elisabeth Musil, Dr. John Hannon, and Dr. Franz Gottleib, for their leadership and expertise. I am thankful to the Walden university staff for their counsel. I also want to acknowledge this study's participants for their time and valuable contribution to the body of business knowledge. I am grateful for my Walden University DBA cohorts' exceptional support during my learning experience, especially Osagie Edison-Edebor, Mutale Chilangwa Chisela, Elizabeth Davis, Dr. Ira J. Phillip Jr., Dr. Jasmine Y. Hardy, and Dr. Dalinda Milne.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Credit card payment constitutes a central part of the e-commerce payment system (Kalbande, 2019), representing a substantial global business growth opportunity. The increased e-commerce traffic makes online credit card fraud opportunities available to more than 20 million online businesses and over two billion individuals worldwide (Pabian et al., 2020). Online card fraud is a criminal activity with a full-scale underground economy (Cai et al., 2018), with no geographic bounds (Cross, 2020), that targets customers (Abdulai, 2020; Mesch & Dodel, 2018), banks, and businesses (Fiore et al., 2019). Online credit card fraud has important consequences for online businesses because a secure online transactional environment is the foundation of a viable global payment system (Kolodiziev & Kotsiuba, 2019).

Regulating and securing an online transaction environment is filled with challenges due to the complexity of the credit card fraud problem (Zanin et al., 2018). The solutions for securing online transactions require a sophisticated and multifaceted approach (see Koraus et al., 2019). Business leaders face important problems due to online credit card fraud, but there is a lack of research addressing leadership strategies to mitigate online fraud. Online card fraud mitigation research primarily focused on exploring prevention technologies (Forough, & Momtazi, 2021; Khattri et al., 2020; Makki et al., 2019; Minastireanu & Mesnita, 2019), cost-efficient technologies (Mekterovic et al., 2021; Olowookere & Adewale, 2020), and transactional risks (Guo et al., 2018). Leadership mitigation strategies are important because securing and

maintaining customers' trust and reducing financial losses involves leaders preventing, detecting, and responding to fraud risk in an agile manner. The purpose of this research study was to explore strategies business leaders use to mitigate online credit card fraud.

Problem Statement

Credit card fraud causes the loss of millions of dollars from the United States economy every year (Downing et al., 2018). Financial losses due to online credit card fraud increased by 127% from 2017 to 2020 (Federal Bureau of Investigation [FBI], 2018, 2019, 2020, 2021). The general business problem is the loss of revenue due to online credit card fraud. The specific business problem is that some online business leaders lack successful strategies to reduce online credit card fraud.

Purpose Statement

The purpose of this qualitative multiple case study was to explore how online business leaders successfully mitigate the loss of revenue caused by online credit card fraud. The targeted population consisted of five online business leaders in the Southwest United States region who have successfully implemented strategies by demonstrating reduced revenue losses due to online credit card fraud. The implications for positive business impact include illustrating examples of successful strategies online business leaders use to prevent and mitigate online credit card fraud, retain consumer confidence in online transactions, and stimulate economic growth. The implications for positive social change include the potential to maintain consumer confidence in e-commerce and reduce consumers' collateral damage of credit card fraud.

Nature of the Study

The three main research methods are qualitative, quantitative, and mixed methods (Baskarada & Koronios, 2018). I selected the qualitative research method to understand and explore the detailed accounts the participants experienced strategizing against online credit card fraud. Researchers use the qualitative method to explore the issue illustrated by the case (Yin, 2018). The quantitative research method is used by researchers to analyze phenomena according to numerical data (Strijker et al., 2020). I did not select the quantitative method for this study because investigating variables relationships or group differences through statistical testing hypotheses would not support the purpose of developing a deep understanding of the question intended to address in the study. The mixed research method combines the techniques from at least one qualitative and one quantitative approach in collecting, analyzing, and reporting findings (Alavi et al., 2018). I did not choose the mixed method for this study because the quantitative component of the mixed methodology was not necessary to answer the proposed research question.

The three qualitative research designs that I considered for this study were: phenomenological, ethnographic research, and case study. Researchers use the phenomenological research design to investigate the personal meanings individuals give to a lived experience about a phenomenon (Kegler et al., 2019). I did not choose a phenomenological research design for this study because I intended to explore individuals' experiences in the context of the phenomenon instead of focusing the investigation on the personal meaning of experiencing the phenomenon. Researchers using ethnography investigate race, cultural practices, and social relations (Magnat,

2018). Ethnographic research was not the best option for this study because I did not intend to analyze or interpret social dynamics. Researchers who use a case study design do an in-depth explanatory, exploratory, or descriptive investigation of a case within its environmental context (Mishra & Dey, 2021). Bansal et al. (2018) stated that multiple case studies logics a comparison of similarities and differences among cases. Therefore, I selected a multiple case study design to create direct replications from case to case to compare the similarities and differences among cases. A multiple case design was appropriate for this research because it was suitable for gathering information that could enhance the knowledge about various successful online business leaders' strategies to mitigate credit card fraud.

Research Question

What successful strategies have online business leaders used to reduce revenue loss from credit card fraud?

Interview Questions

1. What are the successful strategies and security tools you used to reduce online credit card fraud?
2. What method(s) did you find work best to measure the success of your strategy?
3. What internal or external critical success factors did you consider in the design of your strategy?
4. How did you address the key obstacles in the implementation of your strategy?
5. What additional information can you share regarding your organization's experiences with strategies for reducing online credit card fraud?

Conceptual Framework

The conceptual framework for this study was the situational crime prevention theory (SCP). The SCP, developed in 1970 by the British government's criminological research department under the leadership of R. V. G. Clarke (Clarke & Cornish, 1985), is the seminal theory for reducing opportunities for crime. By using the SCP theory, practitioners focus on a crime setting, not on the perpetrator of the criminal activity (Clarke, 1980). Clarke argued that SCP is useful in specific categories of crime by manipulating the environment to minimize the opportunity for illegal activity or magnifying the perception of negative consequences for such crime. The SCP theory refers to the idea that individuals will take advantage of an opportunity to commit an offense if the anticipated benefits exceed the expected consequences (Clarke, 1983).

The SCP theory is useful for identifying circumstances that facilitate criminal activity and restrict those opportunities, motivations, or rewards for committing a crime (Clarke, 1983). The five leading critical activities of prevention are (a) increase effort, (b) increase risk, (c) reduce rewards, (d) reduce provocations, and (e) remove excuses (Cornish & Clarke, 2003). The SCP theory implementation's success depends on surveillance and control over the area prone to criminal activity. The SCP theory was appropriate for this study because it was relevant to the subject under analysis. Managers can apply the SCP theory to avoid illegal activities such as property theft (Simmons, 2018).

Operational Definitions

Account takeover: This occurs when the fraudster accesses further information about the cardholder illegally. The fraudster contacts the cardholder's issuing bank posing as the cardholder provides the information required to get more details about the user to withdraw funds, make illegal transactions, and change account details (Singh & Jain, 2020).

Anomaly detection: Methods focused on detecting and filtering any incoming transaction inconsistent with the cardholder's profile (Jiang et al., 2018).

Card-not-present fraud: In this type of fraud, the fraudster obtains stolen card information for unauthorized use (Singh & Jain, 2020).

Classifier-based detection: Supervised learning methods used to train a classifier on extracting fraud features from fraud transactions (Jiang et al., 2018).

Credit card fraud: The act of obtaining unauthorized funds from an account using a payment card as a fraudulent source of funds in a transaction (Manlangit et al., 2019).

E-commerce: An abbreviation for electronic commerce, which involves buying and selling goods and services over the internet (Zuo, 2021).

Problem of concept drift: The undetectable fraud features due to fraudsters' seasonality and new attack strategies (Jiang et al., 2018).

Skimming: Illegal collection and transfer of magnetic strip information from a payment card to a duplicate virtual or physical card for fraudulent distribution or use while the cardholder is near the location making a purchase transaction (Shulzhenko & Romashkin, 2020).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are ideas accepted as plausible without the proof of developed findings or valid research (Levitt et al., 2021). I had three assumptions in this study. My first assumption was that the participants understood the interview questions and accurately recalled their experiences. My second assumption was the participants answered interview questions truthfully. My third assumption was the participants were willing and prepared to provide supporting documentation of their statements.

Limitations

Limitations indicate areas of uncertainty that a researcher identifies within a research study but cannot address (Munthe-Kaas et al., 2018). I recognized two main limitations to this study. The first limitation was the participants' confidentiality agreements with their organizations could have limited the amount of information they could disclose. The second limitation was the data collected might have not adequately represented the experiences of all online business leaders who have implemented an online prevention strategy against credit card fraud.

Delimitations

Delimitations are the parameters of the study set and controlled by the researcher to narrow the focus of the study (Alpi & Evans, 2019). I identified four delimitations in this study. The first delimitation was leaders who have implemented online mitigation strategies against credit card fraud participated in the research. The second delimitation was leaders with more than 5 years of experience in online fraud mitigation strategies

participated in this research. The third delimitation was the participants of organizations with over 500 employees. The fourth delimitation was participants located in the Southwest region of the United States.

Significance of the Study

The internet facilitates an environment where businesses, customers, and fraudsters can interact (Cross, 2018). In the United States, business leaders absorb the total liability of fraudulent transactions (Guo et al., 2018). Online credit card fraud can drive an increase in the risk of closing a business and reducing customers' traffic. The findings of this study illustrated examples of successful strategies used by online business leaders to prevent and mitigate online credit card fraud, retain consumer confidence in online transactions, and stimulate economic growth.

Contribution to Business Practice

The results from this study can be used by online business leaders to gain insight into practical ways for setting up procedures and practices for the early detection and mitigation of online credit card fraud. Practitioners could also use this information to implement processes that support the integrity of online commerce. The findings from this study can contribute to business practice by providing examples of successful strategies used by online business leaders to reduce the loss of revenue due to credit card fraud.

Implications for Social Change

Online credit card fraud endangers the online payment system and deteriorates customers' confidence in online shopping (Ryman-Tubb et al., 2018). According to

Jordan et al. (2018), fear of financial losses and reputational damage enhances risk perception and decreases customers' intention to make online purchases. The conclusions of this research may catalyze positive social change by potentially helping customers retain or gain confidence in online shopping. Other consequences of identity fraud include a significant psychological toll and physical problems (Randa & Reyns, 2020) that are far-reaching and longstanding (Choi et al., 2021). The findings of this study could increase consumer peace of mind by helping businesses improve systems by enhancing consumers' protection. In addition, reducing revenue loss from fraud could make resources available to improve the human condition by redirecting resources to community programs for developing individuals by teaching and empowering them with control over their financial information during online transactions.

A Review of the Professional and Academic Literature

In this literature review, I explored the SCP used as the conceptual framework for this study. In this literature review, I discuss the theory's evolution, supporting and contrasting theories, critical analysis, and synthesis of related peer-reviewed articles on research studies supporting the SCP theory. By reviewing the content, I provided an overview of online credit card fraud, mitigation strategies, and the impact of this type of fraud on online business revenue. Furthermore, I evaluated, analyzed, and summarized the material related to my research question and compared the research study sources. The purpose of this research study was to learn about successful strategies online business leaders have used to reduce revenue loss from credit card fraud.

I obtained the research materials from Walden University Library's website, University of Texas Library's database, Google Scholar, Criminal Justice, Criminological Highlights of the University of Toronto, EBSCO's Business Source Complete, SAGE Premier, EBSCO, ProQuest, and other databases that contain peer-reviewed articles. I verified the peer-reviewed status of the reference journals with Ulrich's Periodicals Directory. I researched keywords and phrases relevant to the SCP theory.

The keywords I used for searches are cybersecurity, financial crime, leadership online credit card fraud, organized online credit card crime activity, organized crime, rational choice theory, SCP theory, and strategic approaches to crime prevention. This study contains 220 sources, of which 90.4% are peer-reviewed publications. A total of 188 of the 220 sources, 85.45%, were publications between 2018 and 2022.

Situational Crime Prevention Theory

Online financial transactions are convenient for individuals and efficiently improve the quality of banking and business services. The convenience online financial transactions provide customers includes opportunities for fraudsters to abuse and exploit vulnerabilities in the internet financial transaction process. Exploitation by fraudsters causes monetary losses for online businesses and customers (Hussein et al., 2021). Due to online credit card fraud, there were reported losses of over $57 million in the United States during 2017 (FBI, 2018) and over $129 million in 2020 (FBI, 2021).

The implementation of antifraud controls is challenging due to the unique characteristics of the internet. The online environment complicates cybercrimes' intervention, determent, and prosecution because of user negligence, shifts in fraud

schemes, lack of centralized governance, geographical boundaries, or jurisdictional limits (Cross, 2020). Levi (2017) presented a gap in identifying appropriate metrics for judging the threats, the harm from cybercrimes, and their impact on security. Applying the appropriate theories for crime prevention is necessary to develop a successful crime prevention strategy (Welsh et al., 2018). A significant amount of research supports the SCP theory's effectiveness and success in fraud prevention strategies (Prenzler, 2019).

The SCP development occurred under R. V G. Clarke's leadership during the 1970s in the Home Office Research Unit of the British government's Criminological Research Department (Clarke & Cornish, 1985). The researchers in this unit reviewed several forms of crime control and concluded that immediate situational influences play an essential role in criminal activity. Their research findings showed that criminal conduct was susceptible to opportunity, transitory pressures, and incentives. A central tenet of SCP is that opportunities for illegal activity in the environment may be more predictive of criminal activity than criminal tendencies (Cook et al., 2018).

The idea of the SCP originated in the works of Jacobs' (1961) and Jeffery's (1971) crime prevention through environmental design, Newman's (1972) defensible space, and Goldstein's (1979) problem-oriented policing. Jacobs identified the importance of designing safe and secure streets. A safely designed city contains clear delineations, surveillance, and a large neighborhood watch group (Jacobs, 1961). Through crime prevention through environmental design (CPTED), Jeffery's (1971) crime prevention incorporated the importance of considering the genetic predisposition and the physical environment to crime prevention design. CPTED approaches to address

crime from a multidisciplinary perspective because the causes of crime involve social, behavioral, political, psychological, and biological components and influences.

The defensive space theory describes a system in which neighborhoods' architectural design is used to determine the factors in criminal activity incidence (Newman, 1972). The defensive space framework incorporates territoriality, surveillance, image management, access control, and geographical coordination to control, defend, and deter crime (Piroozfar et al., 2019). Newman (1972) argued that the defensive space framework's application would promote a sense of ownership, community, and responsibility in residents, which would motivate them to secure their neighborhoods.

Problem-oriented policing is a police management process that seeks operational efficiency using preventive crime strategies (Goldstein, 1979). Under this approach, the evaluator defines the problem by taking an in-depth look at factors such as the type of problematic behavior, kind of place, people involved, and the time of the crime (Scott, 2018). The information gathered from the scrutiny of the problem creates subsequent strategies against criminal activity and improves policing. Problem-oriented policing prevention strategy includes altering physical environments to reduce criminal opportunities, mediations, and collaborations with community organizations (Scott, 2018).

According to Clarke (1983), individuals take advantage of opportunities to commit a crime if the anticipated benefits exceed the expected consequences. The SCP framework does not support differentiation between criminal and noncriminal individuals (Clarke, 1980). Investigators do not use SCP to eliminate delinquent tendencies or detect

criminals. SCP techniques attempt to make the crime scene unattractive to the offenders based on the level of difficulty or lack of reward (Clarke, 1980). The increase in security measures and the decrease in the benefits of committing a crime should influence individuals to choose against committing the crime. SCP strategies include setting up standards that reduce the opportunity to commit a crime, managing the immediate environment, and elevating risk levels. Some illustrations of SCP are surveillance cameras, restricted access to neighborhoods, and passwords.

Investigators use the SCP framework to understand how individuals take advantage of opportunities to commit a crime (Freilich et al., 2018). Investigators use the inspection results to improve previous strategies to reduce crime opportunities. Cornish and Clarke (2003) developed 25 techniques to reduce opportunities for crime. The techniques fall into five categories: increasing the risks of getting caught, increasing the effort required to commit a crime, reducing the rewards of crime, reducing provocations to commit a crime, and removing excuses for committing the crime. The objective of implementing SCP techniques in real-life settings is to limit, deter, and identify criminal activities.

Significance of Situational Crime Prevention

Researchers study financial crimes by using the lens of moral theories (Lokanan, 2018). According to Lokanan (2018), moral values are a significant factor in criminal activity. Some criminological theories explain why psychological, social, or biological traits influence some groups or individuals to commit crimes. In contrast, investigators of the SCP design observe the situational determinants of a crime because motivation is not

enough of a drive for an offense; there has to be an opportunity to undertake the criminal act. Criminal behavior is more likely to be repeated when the outcome is rewarding for the perpetrator (Clarke, 1980). Controlling delinquent behavior by manipulating immediate opportunities has demonstrated an effective tactic for blocking diverse types of crimes such as terrorism (Freilich et al., 2018), maritime pirate attacks (Shane et al., 2018), organized crime (Korsell, 2018), sexual offenses against women (Chiu et al., 2021), public mass violence (Freilich et al., 2020), cyber-theft and cyber-trespassing (Chavez & Bichler, 2019).

Opportunistic and calculated crimes are highly susceptible to their situation (Clarke & Cornish, 1985). Effective crime prevention strategies depend on the careful analysis of the environmental circumstances of the offense. Consequently, designing out opportunities for criminal activity using the environment given. Cook et al. (2018) showed that sexual offenders decide to commit sexual assault depending on the offender's perception of the immediate situation's security level. Appropriately designing the environment to increase the difficulty of engaging in criminal activity or denying the rewards could influence individuals' decision-making (Clarke & Cornish, 1985).

Previous researchers have used the SCP framework to cover a broad range of individuals, groups, institutions, and governments (Brantingham et al., 2005), and it is compatible with other prevention criminological frameworks. Chavez and Bichler (2019) examined the efficacy of SCP on several cybercrimes by adopting methods used by hackers to counter online victimization. The results showed that increasing efforts and reducing rewards were the frequently recommended prevention strategies. Findings also

showed that novice computer skills individuals could implement 90% of the recommendations. Safa et al. (2019) incorporated deterrence and SCP theories to handle information security insider threats in organizations. Safa et al. (2019) validated the reliability and efficacy of the proposed framework. Simmons (2018) applied routine activity, rational choice, and SCP theories to help librarians control criminal activity in an academic library. The implementation was successful and cost-efficient to execute (Simmons, 2018). Paraskevas and Brookes (2018) designed a framework for disrupting the trafficking of human beings in the hotel sector using the crime pattern theory (CPT), deterrence theory, rational choice theory (RCT), and routine activity theory (RAT). The study's findings showed that the framework of the trafficked victim's journey is effectively applicable to the tourism industry sector to prevent the trafficking of human beings (Paraskevas & Brookes, 2018).

Strengths of Situational Crime Prevention

The SCP framework is an evidence-based scientific approach to understanding and resolving delinquency problems (Mihinjac & Saville, 2019). Investigators use the SCP framework for in-depth examination and disaggregation of the crime scene, which provides appropriate strategies against criminal activity. The SCP framework is narrow, specific, and applicable broadly and systematically (Felson, 2018). SCP researchers have accumulated many examples of preventive ideas, empirical studies, and data for many criminal situations and various parts of the world, supporting SCP efficacy (Felson, 2018).

Limiting the opportunities and manipulating the perception of the situation may discourage or prevent potential offenders from engaging in delinquency (Clarke, 1980). Individuals rationalize taking advantage of an opportunity to commit a crime if they perceive a more significant gain than a loss. SCP techniques focus on blocking opportunities for criminal activity. Olivero et al. (2019) showed that numerous people of different genders and age groups committed digital piracy when the opportunity became available. Olivero et al. (2019) supported more effective interventions to prevent digital theft.

The SCP model is adaptable to the region, context, and immediate environment under intervention (Freilich et al., 2018). Strategies that work well in the United States may not be relevant in another geographic region or vice versa (Freilich et al., 2018). Identifying the routines, patterns, and immediate factors that influence human criminal activity is central to the construction of any situational intervention (Brantingham et al., 2005). Freilich et al. (2018) found that applying the SCP interventions to terrorist groups effectively tailored the SCP to the specific geographical situation. Terrorist groups face different opportunities than other groups in other regions due to varying government regulations and access levels to weapon types, resources, and tools (Freilich et al., 2018).

Limitations of the Situational Crime Prevention Theory

Some theorists questioned the theoretical competence and others focused on the ethical foundation of SCP. Some theorists viewed the SCP as not grounded in crime and offensive etiology because the SCP is not used to focus on the offenders (Hayward, 2007). Some researchers argued that the SCP theory might be defective because the basis

on which the theory attempts to prevent crime fails to recognize criminality's social, cultural, and emotional aspects (Hayward & Hobbs, 2007). Other researchers claimed that SCP techniques risk being exclusionary and ugly, threaten privacy, jeopardize citizens' civil liberties, and blame the victims (Tilley, 2018). Clarke (1980) argued theoretical approach, such as SCP, might provide a higher and more representative perspective on crime prevention.

The implementation of the SCP techniques is not infallible. The determined or emotionally aroused individual may employ countermeasures outside the SCP strategy scope (Clarke, 1980). The efficacy of SCP is not in question for its failed implementations; instead, it suggests that criminal behavior is a complex issue that requires further investigation (Leclerc & Savona, 2016). SCP framework's applicability to countermeasures techniques requires further systematical evaluation (Cook et al., 2018).

A further constraint on the implementation of SCP strategies is the financial cost. Implementing crime control can be complex due to implementation and maintenance costs (Tilley, 2018). Some business leaders that could reduce crime by applying SCP to the prevention solution considered that implementing situational prevention strategies would not be worth the expense (Clarke, 1980). Some business leaders believe that some level of crime may be an inevitable consequence of business practice, and the cost of crime prevention strategies may not be considered reasonable (Tilley, 2018). Several cost-sensitive models have demonstrated strong evaluation metrics while keeping a low

cost (Singh & Jain, 2020). Akila and Srinivasulu Reddy (2018) proposed a cost-efficient model that aligns with the business's fraud prevention budget goals.

Supporting Theories

The SCP is a cognate field of study to CPT, deterrence theory, RCT, and RAT. Investigators use this set of theories to evaluate circumstances surrounding a criminal event or the location where the crime occurs. CPT strategies help researchers identify areas prone to illegal activity (Brantingham & Brantingham, 1981). Strategies based on the deterrence theory aim to discourage the individual from committing a crime (Beccaria, 1764). RCT crime prevention efforts make criminal activity unappealing to the individual based on opportunity cost (Cornish & Clarke, 1986). RAT strategies focus on removing opportunities for a crime in the social and physical environment (Cohen & Felson, 1979).

Brantingham and Brantingham (1981) developed CPT, which asserts that physical and social environments may facilitate criminal occurrences based on the offender's familiarity with the location and the opportunity to commit the act. Under this perspective, offenders commit criminal activity in the locations they know because they learn about crime opportunities while spending time in areas they go about in their daily routines. Menting (2017) studied interactions between offenders' awareness and opportunity. The study results confirmed that familiarity with the location and opportunity for fraud are essential factors in predicting the place for a crime (Menting, 2017). Summers and Johnson's (2017) results showed predatorily (planned) and spontaneous (unplanned) crimes may occur in places that are familiar to the offender. The

CPT approach has proven effective in understanding crime and its location (Hewitt et al., 2018).

Beccaria (1764) founded the deterrence theory, sometimes called rational deterrence theory, in which he argued that punishment proportionate to the crime would persuade individuals to avoid criminal behavior. Deterrence theorists believe that the punishment or sentence for a crime would influence criminals' decision not to commit a delinquent act (Lupovici, 2019; Taddeo, 2018b). Safa et al. (2019) found anticipated sanctions significantly reduced employees' engagement in information security misconduct. Taddeo (2018a) argued that deterrence is helpful for crime prevention. Still, a successful cybersecurity deterrence requires the deterrence strategy to focus on prevailing against further attacks or retaliation attacks instead of just threatening against attacks. Wilner (2020) stated the scope of cyber deterrence theory should include the array of variables within the internet environment.

Bentham (1789) made contributions to Beccaria's (1764) deterrence theory, including the notion of making a rational choice between pain and pleasure of committing a crime. Bentham argued that an individual is more likely to commit a crime when pleasure counterbalances the pain. Bentham's (1789) expansion of the deterrence theory was later named the RCT. Cornish and Clarke (1986) migrated the RCT into criminology to address crime control by understanding the individuals' decision-making process of engaging in a criminal act. Individuals make decisions based on the advantages surpassing the costs of committing a crime (Cornish & Clarke, 1986). RCT theorists saw criminal impulses as an inherent nature of humanity, and individuals with

low self-control are more likely to commit a crime. Charki et al. (2017) researched the impact of legal punishments on mitigating unethical information technology use. Although mitigation was part of the outcome, the study results showed that new unethical information technology use cases emerged, and some users disengaged from technology use. Charki et al. (2017) concluded that successful strategies for unethical information technology using mitigation include an evolving combination of mechanisms that combine different types of users and stakeholders. Li et al. (2018) researched factors influencing internet use policy compliance at the workplace. The results showed that mitigating noncompliance with internet use policy depends on the individual's perspective.

Cohen and Felson (1979) collaborated on the RAT, sometimes referred to as lifestyle theory, to explain situational factors that influence participation in crime, such as motivation, opportunity, and security. Researchers do not use RAT to focus on the criminals but on how changes in social activities and the environment may trigger individuals' criminal tendencies and present opportunities for crime. Cohen and Felson (1979) argued a convergence of a motivated offender, a suitable target, and lack of security creates vulnerability for illegal activity. As the perception of the opportunity for rewards and benefits increases, criminal behavior's propensity becomes greater. The RAT's elements support researchers' crime prevention efforts by predicting the conditions where criminal activity is prone to occur. Researchers have successfully applied the RAT framework to a variety of scenarios (Ming-Li & Shun-Yung, 2018), such as online chief executive officer fraud (Junger et al., 2020), website defacement

victimization (Howell et al., 2019), school bullying (Cho & Lee, 2018), and adolescent sexual revictimization (Culatta et al., 2020).

Contrasting Theories

Some of the contrasting views from the SCP are the proponents of the theory of crime displacement, the labeling theory, and the social learning theory (SLT). These theories lay the foundation for evaluating individuals' sociological, biological, and psychological dispositions to commit the crime. These qualities are the primary determinants and influencers of engaging in fraudulent activity.

Theorists use the crime displacement established by Reppetto (1976) to explain the relocation of criminal activity due to crime prevention interventions. According to Reppetto (1976), crime prevention strategies do not affect illegal activity because criminals respond to intervention by adapting and modifying the crime, target, method, place, or criminal activity time. Ladegaard (2019) applied the crime displacement theory to illegal digital drug trade websites and online networks after police intervention. The findings of this study showed that the fraud relocated to new illegal digital drug sellers' websites. The results also showed the fraudsters reorganized and created new online networks with improved technologies. Z. Wang et al.'s (2019) research results showed that crime displacement does not move far away from the displaced location.

The labeling theory created by Tannenbaum (1938), expanded by Becker (1963), and advanced by Braithwaite (1989), explains a possible consequence of social controls. According to Becker (1963), deviant behavior resulted from the labels created by society's ruling powers. The individual develops a negative self-concept based on being

labeled a criminal by the judicial system and subsequent deviant behavior (Tannenbaum, 1938). Due to life reintegration challenges, the individual engages in crime reoccurrences (Braithwaite, 1989). Labeling is a form of public shaming that tends to be ineffective because the stigma degrades individuals (Braithwaite, 1989). Stigmatizing offenders often isolates them from social groups and increases the probabilities of subsequent criminal acts. Braithwaite (1989) claimed the labeling theory highlights the relationship between effectively communicating shame about crime and lower crime rates. Kroska et al. (2017) researched the relationship between labeling theory, self-meaning, and juvenile delinquency. The findings showed that labeling promotes engagement in deviant behavior.

Burgess and Akers (1966) developed the SLT based on Sutherland's (1938) differential association theory concepts. According to Sutherland (1938), individuals engage in a crime because they learn criminal behavior through communication with an intimate group of individuals that engage, have tendencies, or support deviant behavior. Sutherland argued that interactions with primary criminal groups are not enough to motivate a person to become a criminal. Adopting, imitating techniques, rationalizing illegal activity, developing a motivation to commit a crime, and calculating a crime's reinforcers require an unbalanced favorable view of offending (Sutherland, 1939). Similarly, the proponent theorists of social learning state that criminal learning behavior occurs in an intimate group of individuals with inclinations, engagement, and criminal behavior support (Akers, 1998). Individuals commit a crime not because of opportunities but because of bias and learned skills of deviant behavior. Ward et al. (2018) examined

the differences in theoretical integration and explanation capabilities of the social learning and social control theories in adolescents' alcohol use. Ward et al. (2018) found social learning processes greatly influenced individuals' behavior.

Defining the Business Problem

During the 1920s, card payment processing occurred on "charga-plate" imprinter machines (Lauer, 2020). The zip-zap device was convenient because it allowed customers access to their funds without carrying currency. The charga-plate machine transaction processing took days to pay the merchants and generated multiple carbon paper copies, which facilitated fraudsters' ability to obtain a copy and misuse card information (Lauer, 2020). The magnetic strip replaced the use of the charga-plate machine in the 1980s (Lauer, 2020). The payments to businesses were deposited within hours, reducing the visibility of card information on paper receipts and the number of paper copies per transaction. The magnetic strip posed a significant vulnerability to the payment system (Pigni et al., 2018) for fraud (GieBmann, 2018), such as card skimming (Singh & Jain, 2020).

Incorporating the Europay, Mastercard, and Visa (EMV) card chip reader system for in-person transactions helped decrease the risk of counterfeit transactions (Sportiello, 2019). The EMV card avoided the security issues posed by the magnetic stripe cards (Olowolayemo et al., 2019). Customers insert their chip card in the card reader during in-person purchases to communicate with the system to process the charge (Sportiello, 2019). The EMV technology secured transactions by using the embedded cardholder's card and personal information in the card's microchip with a point of sales equipment to

generate a unique one-time code per transaction unuseful if counterfeited (Olowolayemo et al., 2019). Fraudsters have identified and exploited weaknesses in EMV technology (Al-Maliki & Al-Assam, 2021). Business leaders that upgraded their payment system to accept the chip reader on card-present payment transactions could shift the fraud's liability to the bank. Business leaders who do not upgrade their payment system to accept the chip reader absorb the total cost of card not present fraud. The Europay, Mastercard, and Visa chip technology helped reduce the risk of fraudulent charges at business establishments (Olowolayemo et al., 2019), but not for online purchases, where card fraud is on the rise.

The credit card payment processing involves the cardholder, issuing bank, payment processor, fraud security team, and business owner's bank. The cardholder inserts the card information on the website for online purchases during in-person purchases. The business representative sends the inserted card details to the business owner's bank (Nasr et al., 2020). The business owner's bank forwards the information to the payment processor network that electronically communicates with the issuer fraud team and waits for the transaction to become verified as legitimate. Upon approval, the bank transfers the transaction amount to the business' bank. When the transaction turns out to be unauthorized by the cardholder, the customers' issuing bank refunds the cardholder the unauthorized charge and then withdraws the transaction amount from the business's acquiring bank account. The business owner cannot stop the issuing bank from withdrawing the funds from the acquiring bank account. Under qualified circumstances, the business owner can submit a dispute to the issuing bank for consideration. The

business owner pays chargeback fees to credit card companies (Guo et al., 2018). Chargebacks incur variable fees that depend on the claim amount or flat-fee penalties, which are constant regardless of the claim amount (Chen, 2018).

Types of Credit card Fraud

The main types of credit card fraud are counterfeit cards, chargeback or friendly fraud, merchant fraud, and card not present fraud. A counterfeit card is the unauthorized duplication of credit card information from the original card to a blank card (Vargas, 2019). Fraudsters gather unauthorized personal information from credit cardholders in a variety of methods such as finding a lost credit card, stealing the physical card, or obtaining credit card information via phishing (O'Leary, 2019), a pseudo base station (Yu, 2019), skimming attack (Al-Maliki, & Al-Assam, 2021), malicious insider (Kim et al., 2019), credit card cloning (Vargas, 2019), phishing, and external interactive voice response systems fraud (Kolodiziev & Kotsiuba, 2019). A chargeback or friendly fraud happens when a merchant is required to issue a refund to a charge that a customer claimed is not authorized (Guo et al., 2018). Merchant fraud refers to inside business fraud activity by a staff member. Card not present fraud occurs when an unauthorized user makes fraudulent transactions while not physically present at the business establishment (Singh & Jain, 2020).

Credit card Fraud Mitigation Strategies

Online credit card fraud-fighting strategies are reactive, proactive, or a combination of reactive and proactive (Saia & Carta, 2019). Reactive strategies are the initiatives that come into effect after the crime occurs, such as blocking the stolen card to

prevent further unauthorized charges. Proactive approaches such as fraud authentication tools prevent crime (Saia & Carta, 2019) and help identify the customer's information and verify a transaction's validity (Sadgali et al., 2020). Some examples of authentication tools are card verification code and address verification systems. The card verification code is the three-digit string of numbers located on the back of the card. Card verification is a useful tool but lacks protection when fraudsters get a hold of the credit card details (Sadgali et al., 2020). Investigators use the address verification system to validate transactions by verifying the cardholder's address. The address verification system cannot prevent fraudulent charges when the fraudsters access the cardholder information from bank files (Sadgali et al., 2020) or public data. A reactive and proactive strategy can help design a robust fraud mitigation solution (Saia & Carta, 2019).

The stages of fraud prevention strategy include: (a) prescreen, (b) payment, (c) post-screen, (d) review, and (e) accounting. During the prescreening stage, the order information undergoes a review process to assess the business's capacity to fulfill the order. Business leaders assess the order or service availability in the prescreening stage. The payment stage refers to the features and tools used to process the charge. The post-screen phase is an in-depth transaction review. A manual review of the transactions' history queue occurs in the review stage. The accounting phase involves handling order discrepancies within 12 months of the transaction, such as chargebacks and reauthorizations. The level of business risk determines the required number of fraud prevention strategy phases needed for a fraud solution (Montague, 2010).

Business leaders may consider eight fraud solution providers as part of their fraud solution strategy: guarantee fraud-solution providers, identity providers, fraud-scoring providers, shared network providers, technology providers, analytic providers, data quality providers, and operational providers (Montague, 2010). According to Attigeri et al. (2018), the most beneficial strategy for business leaders matches the business model. It also considers several factors such as fraud rate, consumer transaction abandonment rate, business profit margin, and average transaction value. Business leaders should assess their business risk level and the financial resources available to decide if they should hire providers and, if so, which service providers are necessary to handle their fraud prevention challenges.

Obstacles to Credit Card Fraud Detection and Prevention

The challenges associated with credit card fraud prevention present an important risk for organizations (Jurgovsky et al., 2018). Online business leaders should look out for regular offenders, criminal offenders, and organized crime. Regular offenders are the customers that engage in fraudulent activities against a business, such as chargebacks and misrepresentation of application details (Amasiatu & Shah, 2019). Criminal offenders are the individuals who intentionally exploit vulnerabilities in business systems for stealing (Ali et al., 2019). Organized crime refers to the industrialization of access to tools for committing criminal activity, such as criminal rings operating in the dark web (Vargas, 2019). Online credit card fraud is an economically lucrative opportunity appealing to criminal offenders (Ali et al., 2019), organized crime (Vargas, 2019), and regular

offenders (Amasiatu & Shah, 2019). Recognizing these types of fraudsters scheming against online businesses is an important step in developing appropriate fraud solutions.

Financial loss due to online credit card fraud increases because of the progressive growth of online payment transactions (Jurgovsky et al., 2018). The high demand for transactions review could exceed the fraud team's processing capacity (Giannini et al., 2020). Large businesses' transaction volume does not allow the fraud team to verify every single cardholder (Nascimento et al., 2019). For an organization of over $1 billion in annual revenue, the average number of unauthorized charges is usually less than 0.1% (X. Zhang et al., 2019). A small percentage of transactions in the queue get compared to the number of authorized charges (Fiore et al., 2019). This imbalance exacerbates the challenge of identifying the unauthorized charges mixed with legitimate payments. At first glance, 0.1% might seem like a small portion of fraudulent activity, but it translates to millions of dollars' annual financial losses (X. Zhang et al., 2019). Credit card financial losses due to credit card fraud in 2020 were $129,820,792 (FBI, 2021). Some techniques proposed to address this discrepancy are oversampling (Manlangit et al., 2019) and under-sampling (Hu et al., 2019).

The resources necessary to address fraud can be costly for a business (Poole et al., 2018), and fraud prevention is ongoing (Richardson, 2020). Preventing fraud requires an investment, and business leaders should value the importance of implementing fraud protection (Nadiia & Snizhana, 2020). In addition to the direct financial losses from fraud, a business might experience a decrease in consumers' confidence in online shopping (Daroch et al., 2021) and loss of reputation. Daroch et al. (2021) found the most

significant factor deterring customers from online shopping was concern over online credit or debit cards payment security and lack of trust in online businesses. Online customers trust making payment transactions with companies with a reputation of keeping a secure transaction process (Ghazali et al., 2019). Trust and reputation are fundamental influencers of online shopping.

Crime indicators fluctuate (Khattri & Singh, 2019), and fraudsters are continually changing their attack strategies by exploiting loopholes in technology (Ali et al., 2019) and looking for new ways to commit fraud (Hussein et al., 2021). Deciding not to invest in a business fraud prevention initiative leaves a business with growing vulnerabilities for fraud. Business leaders should consider all the implications of not financing a robust fraud solution. The results from Richardson's (2020) study showed businesses that establish robust online fraud solutions experience fewer losses due to cybercrime.

Cost of Online Credit Card Fraud

Business leaders' costs resulting from card fraud are direct and indirect (P. Wang et al., 2019). Direct business costs refer to the economic damages from online fraud, such as financial loss, operational costs, and stock price drops (P. Wang et al., 2019). Financial losses from the stolen products or services and the reimbursement of charges to the issuing bank can be a significant expense for a business. Financial losses due to online credit card fraud went from $57,207,248 in 2017 to $129,820,792 in 2020 (Federal Bureau of Investigation [FBI], 2018, 2021). Operational costs refer to the disruptions in productivity and operation activity resulting from the crimes (P. Wang et al., 2019). Online data breaches can severely hurt business stock performance (Pigni et al., 2018). A

security breach has resulted in losses of hundreds of millions of dollars, stock value decline, and earnings drop for businesses (Pigni et al., 2018). A business with a market share value decline due to security breaches incurs additional expenses (P. Wang et al., 2019), such as credit monitoring service for the victims and legal fees (Pigni et al., 2018).

The indirect business costs are the damages equivalent to financial losses caused by fraud (P. Wang et al., 2019). Examples of indirect expenses are negative reputation, potential profit loss, loss of external party investments, loss of market competitiveness, employee talent loss, and creditworthiness decline. The success of the online payment industry depends on gaining and maintaining consumer confidence in the payment systems' safety and security (Oghazi et al., 2021). A business's reputation is a critical factor in a consumer's decision about transacting with the business (Daroch et al., 2021). Customers' trust and purchase intention decline if they perceive security risks on a business website (Bashir et al., 2018). Loss of potential profit resulting from fraud is challenging to determine because of the varied types of indirect impacts affecting potential profits. Janakiraman et al. (2018) found that spending from customers who experienced online fraud decreased by 32.45%.

According to Gwebu et al. (2018), the stock market responds negatively to online business breaches. Businesses that experience a security breach may also lose external parties' investments and market competitiveness (Agrafiotis et al., 2018). A business loses market competitiveness due to the direct and indirect costs caused by a breach (Janakiraman et al., 2018). Businesses with inadequate security measures could lose employee talent due to a business's negative reputation (P. Wang et al., 2019). A negative

business reputation might encourage current staff to leave the company and discourage potential talent from joining the organization. Business creditworthiness is crucial for a business's ability to accept cards as a payment method. Businesses with excessive chargebacks could be liable for additional bank fees and credit rating reductions (P. Wang et al., 2019). A credit rating reduction of a business's creditworthiness translates to the business's ability to use credit cards as a payment method. A credit rating reduction can cause further business expenses, such as increased bank transaction fees. Due to fraud, direct and indirect costs could snowball into additional charges, such as increased business insurance costs and loss of productivity costs breach (Janakiraman et al., 2018).

Summary of Previous Investigations

A significant number of research studies have focused on the cloud computing aspect of online credit card fraud prevention and mitigation, such as computer learning algorithms (Dornadula & Geetha, 2019; Manlangit et al., 2019). Cloud computing refers to real-time online access to a network host of services such as database systems, data storage, and applications (Zou et al., 2021). Learning algorithms allow computers to learn input data patterns to use as a model for reference for output (Ucci et al., 2019). Online business leaders rely on supervised, unsupervised, and semi-supervised learning algorithms to assess the risk of transactions fraud to mitigate fraud (X. Zhang et al., 2019).

The supervised learning algorithms accumulate behavioral patterns and assign labels in a database to create a classification model (X. Zhang et al., 2019). When a transaction does not resemble the classification model, the algorithm labels the

transaction as legitimate or fraudulent, depending on other scoring factors (Taha & Malebary, 2020). The supervised learning algorithms are more constraining and expensive than unsupervised algorithms (Domingues et al., 2018). The unsupervised algorithms cluster data into equal groups and then sort the groups according to account user behavior (Singh & Jain, 2020), such as user or transaction historical payment patterns (Taha & Malebary, 2020). The accumulated customer transaction history becomes a model to identify anomalies (J. Zhang et al., 2019). The transactions that do not conform to the established patterns are considered fraudulent charges (Taha & Malebary, 2020). The semi-supervised algorithms combine supervised and unsupervised algorithm techniques (Carcillo et al., 2019), such as graph-based semi-supervised learning (Ansari et al., 2020). Semi-supervised learning algorithms detect anomalies from a small amount of labeled data (Ansari et al., 2020). Carcillo et al. (2019) indicated a successful online credit card fraud strategy should incorporate multiple components.

Amasiatu and Shah (2019) found that adopting a holistic approach to fraud management can lead to superior fraud solutions. A holistic approach includes raising customers' awareness of the costs and consequences of fraud, training employees to identify, and respond to fraud red flags, conducting in-depth investigations, establishing policies focused on reducing the incidence of fraud, and continuous monitoring of fraud solutions (Amasiatu & Shah, 2019). Tripathi et al. (2018) argued that the best way to identify online card fraud is by monitoring and evaluating transaction habits and creating historical data of the customers' purchasing patterns. Priyangaa et al. (2017) claimed that the only way to detect this type of fraud is to analyze the spending patterns of every card

to identify transactions that deviate from legitimate transactions. Nascimento et al. (2019) found that using the cardholder's information combined with sound analysis, credit cardholder's credit score, and human evaluation helped prevent credit card fraud. According to Nasr et al. (2020), businesses should keep informed of fraud trends and collaborate with a trustworthy payment processor. They also recommended companies should encrypt sensitive information and establish strong policies for handling private data. Junger et al. (2020) suggested that business leaders provide their employees with appropriate online fraud prevention training, support, and tools.

Next Step in Solving the Problem

Online credit card fraud presents a fundamental challenge for business leaders, customers, and banks. Although there has been an improvement in fraud detection strategies, fraud still threatens online businesses' financial health (Guo et al., 2018). Challenges presented by credit card fraud are primarily due to the fraudsters' constant cycle of fraud scheme innovations (Manlangit et al., 2019). Fraudsters find ways around fraud prevention tools by being flexible, taking advantage of opportunities (Moid, 2018), and using online services and software applications (Nadiia & Snizhana, 2020). Card fraud mitigation is essential to handle the onslaught of cybercrimes (Ali et al., 2019).

Credit card fraud is an extensive problem due to technological advances, the volume of transactions, and fraudsters' continuous innovations. A secure payment system depends on a reliable and safe authentication system. Business leaders play an important role in protecting consumer data and mitigating financial losses due to fraud. Business leaders should set up proactive measures to decrease fraud opportunities (Gunasegaran et

al., 2018). Gathering the data, sharing knowledge, and understanding potential fraud threats and solutions might help business leaders get the tools and resources necessary to identify, assess, manage online credit card fraud, and limit the severity and the frequency of fraud (Poole et al., 2018). Understanding leaders' experience in fraud prevention and effective strategies is essential for developing reliable fraud solutions, business growth, and a secure payment system (Ali et al., 2019).

Transition

In Section 1, I presented (a) the background of the problem, (b) the problem statement, (c) the purpose statement, (d) the nature of the study, (e) the research question, and (f) interview questions. I discussed this study's conceptual framework, R. V. G. Clarke's SCP theory (Clarke & Cornish, 1985), and related concepts. I defined the terms used in the study. I identified the assumptions, limitations, and delimitations of the study.

In Section 2, I restate the purpose statement. I define (a) the role of the researcher, (b) the participants, (c) the research method and design, (d) the population and sampling, and (e) ethical research. In section 2, I explain (a) data collection instruments, (b) data collection techniques, (c) data organization technique, (d) data analysis, and (e) reliability and validity of the study.

In Section 3, I include (a) presentation of the findings, (b) application to professional practice, (c) implications for social change, (d) recommendations for action, (e) recommendations for further research, (f) reflections, and (g) conclusion.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore how online business leaders successfully mitigate the loss of revenue caused by online credit card fraud. The targeted population consisted of five online business leaders in the Southwest of the United States who successfully implemented strategies by demonstrating reduced revenue losses due to online credit card fraud. The implications for positive business impact include illustrated examples of successful strategies used by online business leaders to prevent and mitigate online credit card fraud, retain consumer confidence in online transactions, and stimulate economic growth. The implications for positive social change include the potential to maintain consumer confidence in e-commerce and reduce consumers' collateral damage of credit card fraud.

Role of the Researcher

According to Yin (2018), researchers are responsible for the research credibility and dependability and accurately capture the participants' experiences. The researchers are the primary instrument of data collection and analysis (Clark & Veale, 2018). Researchers collect information, insights, meanings, values, and participants' perspectives (Peterson, 2019). Researchers also decide the research question, the research sample's composition, and the participants (Ahmad et al., 2019). As the researcher, my role was to investigate the research question, perform interviews, analyze the collected data, link the data to the literature, and frame a compelling argument following the research design and methodology. Researchers disclose their assumptions and biases

while collecting, coding, and sorting qualitative data (Peterson, 2019) and member checking to ensure the research process's integrity (Brear, 2019). Researchers use reflexivity to reduce personal bias, such as apophenia (see Buetow, 2019). According to Karagiozis (2018), researchers should engage in journaling and internal dialog to become aware and manage my unconscious bias. Therefore, I used reflexivity. Unchecked researcher's bias could alter the research findings in favor of the researcher's perspective instead of providing an authentic representation of the participants' experiences (Wadams & Park, 2018). I also used standardized interview protocol, semistructured interviews, and bracketing techniques to minimize personal bias interference, as Wadams and Park (2018) described. I focused on being open-minded and patient during the research process and strived to understand the phenomenon as described by Kalman (2019). I was sensitive and respectful of the participants' rights and created a space to speak openly about their experiences. My role as a researcher included abiding by the principles and guidelines outlined in the *Belmont Report* of respect for persons, beneficence, and justice as described by the Office for Human Research Protection (2018). The *Belmont Report* principles are the foundation of the consent, assessment of risks and benefits, and participants' selection for the study.

I held a role working as an online revenue protection specialist. My job was to identify, prevent, and mitigate fraudulent charges in a pool of thousands of transactions per day for a large online business. During my role as a fraud team member, the experiences and challenges I encountered motivated me to investigate effective strategies to prevent online credit card fraud. I left the position to reduce viewing the data from the

perspective of an online revenue protection specialist. Biases are deflections that misrepresent the participants' experiences in qualitative research projects (Wadams & Park, 2018).

Gathering an accurate depiction of the participants' experiences is essential to qualitative research (Wadams & Park, 2018). I reached out to the potential participants via phone call (Appendix D) and emailed the consent form. I used a semistructured interview technique (Appendix A). I followed an interview protocol (Appendix B) to facilitate the interview process and obtain rich data within the designated timeframe as described by Yeong et al. (2018). Interview questions should get scheduled around the time allocated for the interview and capture rapport with the participants (Hamilton & Finley, 2020). According to Brimbal et al. (2021), rapport influences participants' disposition to participate in the interview process. I conducted the interviews and member checking according to each participant's convenience. I listened carefully to the participants' responses and was attentive to assure the participants understood each question (see McGrath et al., 2019). I was genuinely open and curious about the interviewees' responses and experiences.

Archibald et al. (2019) found that interviews over electronic can improve the in-person interviewing method. Jenner and Myers (2019) found that video calls' quality of datum was as good if not better than in-person interviews. According to Ballena (2021), the quality of interviewing depends on the design of the questionnaire. The interview questions that I designed for this research study underwent the scrutiny of my Walden chair committee to assure appropriate typology. Using a semistructured interview

technique, I presented open-ended interview questions (Appendix A) with additional follow-up questions as appropriate and engaged in active listening to facilitate participants' reporting, as Karagiozis (2018) described. I followed a semistructured interview technique script to keep consistency in the interview protocol (Appendix B). According to Roulston (2018), semistructured interviews within open-ended questions allow direct and open dialog. I transcribed the recordings from the interviews within 48 hours of each interview completion. Via consent form, I notified the participants of the purpose, ethical guidelines, and policies governing this study and their right to free participation as outlined in the Belmont Report (Appendix E). I assessed the potential benefits and risks of participation in this study. I established a secure safeguard of the participants' confidentiality, including the safe storage of information because protecting the confidentiality of the participants is of paramount importance (see Surmiak, 2018). I advised the participants of the guidelines around the access, storage, and use of this study data.

Participants

The optimal strategy for qualitative research is to recruit participants whose experience is relevant to answering the research question (McGrath et al., 2019). I established an inclusion criterion that supported responding to the research question. Participants should have extensive knowledge about the phenomenon under investigation and can best respond to the research question (Capili, 2021). The criteria for participating in this qualitative multiple case study were that the participants: (a) be online business leaders of an organization with 500 employees or more; (b) have experience

implementing successful online credit card fraud solutions, and (c) be located in the Southwest of the United States.

I accessed the organizations via publicly available information on Best Business Bureau and LinkedIn websites. I reached out to potential participants via phone call (Appendix D) and email. I sent the consent form via email. I set up the interviews according to the participants' preferred date and time. I scheduled the first and follow-up interviews according to the participants' convenience. I sent the consent form and included a description of the study's purpose to the participants via email. According to Croix et al. (2018), a good interview is dependent on the interviewee's comfort level. I provided the participants with the research question and interview questions before the interview. I also provided the participants with a 1 to 2 pages summary of the transcripts to review.

According to Hamilton and Finley (2020), the interview's opening sets the interview's tone and influences the data collection process. I opened the interview by sharing my background and professional experiences with the participants. I established a working relationship with the participants by explaining the study's objectives. I was transparent and communicative with the participants to ensure their retention. I also notified the participants that I would provide them with a copy of the study results. According to Gibaldi and Siddiqi (2019), participants want to know the results of the study in which they participated.

Research Method and Design

Research Method

The three main research methods are qualitative, quantitative, and mixed (Erlingsson & Brysiewicz, 2018). I conducted a qualitative study investigating effective leaders' strategies to mitigate online credit card fraud. The qualitative method is appropriate for obtaining rich data on participants' experiences. Researchers use the qualitative method to provide in-depth insights and understand real-world problems (Yin, 2018). According to (Strijker et al., 2020), researchers use the quantitative research method to analyze phenomena according to numerical data (Strijker et al., 2020). Therefore, I did not select the quantitative method for this study because investigating variables' relationships or group differences through testing hypotheses would not have supported developing a deep understanding of the research question. The mixed method includes using techniques from at least one qualitative and one quantitative approach in collecting, analyzing, and reporting findings (Baskarada & Koronios, 2018). I did not choose the mixed method for this study because the quantitative component of the mixed methodology was not necessary to answer the research question.

Research Design

I considered the three qualitative research designs for this study: phenomenological, ethnographic research, and case study. Researchers use the phenomenology research design to investigate individuals' personal meanings to a lived experience about a common phenomenon (Ghaffari & Lagzian, 2018). I did not choose the phenomenological research design for this study because I intended to explore

individuals' experiences in the context of the phenomenon instead of focusing the investigation on the personal meaning of experiencing the phenomenon. Researchers using ethnography investigate race, cultural practices, and social relations (Magnat, 2018). The ethnographic research was not the best option for this study because I was not attempting to analyze or interpret social dynamics. Researchers who use a case study design do an in-depth explanatory, exploratory, or descriptive investigation of a case within its environmental context (Mishra, & Dey, 2021). Although a case study was an optimal design for this study, a single case study was not appropriate for this study because the methodology would not have supported the intention to identify differences and similarities among the cases as described by Bansal et al. (2018). The multiple case design was an appropriate method to obtain rich data on participants' experiences. I used a multiple case design to establish validity and reach data saturation (see Yin, 2018).

Saturation occurs when enough data to reach conceptual depth is collected, and no other themes or insights of the issue are found even with more interviews or cases added (Saunders et al., 2018). According to Saunders et al. (2018), researchers decide further data collection is unnecessary when the researcher recognizes the redundancy of data from the interviews. I interviewed five participants. To ensure data saturation, I used a semistructured interview technique (see Yeong et al., 2018), member checking (see Iivari, 2018), and interviewed participants until no new information emerged or saturation was achieved (see Hennink et al., 2019).

Population and Sampling

The study population is the total number of participants sampled based on selection criteria and their autonomous participation decision. The population for this multiple case study was composed of five participants from different companies who (a) were online business leaders of an organization with 500 or more employees, (b) had successfully implemented fraud solutions, and (c) had a business located in the Southwest region of the United States. A small sample size of participants is adequate for a qualitative research study (Yin, 2018) because the appropriate sample size for qualitative research determination comes from reaching the data saturation threshold (Saunders et al., 2018). Validity depends on the richness of the data provided by the participants instead of the number of participants (Yin, 2018). Online business leaders who successfully implemented fraud solutions provided rich data to answer the research question.

I selected purposive sampling for this multiple case study because I was looking for an in-depth understanding of the inquiry and not reaching empirical generalizations. Researchers use purposive sampling to identify and select participants with characteristics that provide abundant data pertinent to answering the research question (Conlon et al., 2020). Online business leaders with experience implementing successful credit card fraud solutions provided relevant descriptions of their experiences and practices related to this study. I used a semistructured interview technique via Zoom calls or phone calls conveniently for the participant. Zoom is used to securely record and store audio and video content from meetings without routing it to third-party software

(Archibald et al., 2019). According to Li et al. (2019), semistructured interviews promote candid conversations with the participants and facilitate rich data gathering. I used Zoom to perform and record audio call interviews. I advised the participant to select a convenient time to speak at liberty and comfort during the interview.

Data saturation is vital in any study (Guest et al., 2020). Researchers achieve data saturation to ensure that research data are credible, transferable, dependable, and the investigation is confirmable (Yin, 2018). Data saturation occurs when no new data, no new themes, and no new coding are obtained (Moser & Korstjens, 2018). According to Sim et al. (2018), researchers can reach data saturation by asking multiple participants the same questions until no new information is forthcoming or new themes are evident. I used the semistructured interview technique, member checking (Appendix C), business progress reports, and credit rating reports to ensure data saturation.

Ethical Research

The researcher is responsible for compliance with ethical conduct during the study (Cumyn et al., 2019). I provided a safe environment by adopting a transparent process, ensuring the participants were well informed, valued, and not harmed, coerced, or inconvenienced. Embracing information transparency to the participants and maintaining data privacy engages participation and trust (J. Lee et al., 2018). I followed the Institutional Review Board's (IRB) ethical standards by treating the participants with respect, transparency, and fairness. I protected the participants' identities and personal information by limiting specific participant characteristics and coding the participant as P1, P2, P3, and their organization's identity as B1, B2, B3. I also provided the

participants with full disclosure of all relevant information about the study to determine the participant's disposition to participate. The consent form included information about the participants' role, benefits, and potential risks involved in participation (see Metselaar, 2019). I obtained written consent via email from participants by replying, "I consent," to agree to participate in this study. The participants had the opportunity to ask questions before signing the informed consent form via email or call.

All personal data I collected during the interviews remained confidential. The names of the participants and business-related documentation were assigned a pseudo-code composed of a random letter and a number representing the participant's name. Ross et al. (2018) argued that qualitative research is vulnerable to reidentification. Coding the participants' names and responses will keep participants' personal and business identities confidential (see Yin, 2018). I saved all data related to this study in a password-protected thumb drive inside a weatherproof lockbox. As designated by Walden University, 5 years after completing this study, all digital data will get permanently deleted, and the original paperwork related to this study will be mechanically shredded.

According to Yin (2018), the participants should have the opportunity to withdraw from the study at any time. The study participants were free to withdraw from the study with no negative consequences through verbal or written notice expressing their desire to withdraw. I waited to schedule any interviews until I received the consent email from the participant. I did not initiate data collection before receiving IRB approval. Obtaining IRB approval before beginning the research study ensures (a) the study has the

potential to contribute valuable knowledge, (b) the participants' welfare and rights are protected, and (c) the risks inherent in the research study are minute compared to the potential benefit gained from the study (V. Lee, 2018). The IRB number for this study is 08-05-21-0454040.

Some researchers use financial incentives or reimbursement for reasonable expenses to encourage participation in studies (Gelinas et al., 2018). Other researchers encourage participation by motivating the participants to volunteer as an altruistic act (Gelinas et al., 2018). I communicated to the participants their contribution to this research is valuable and might benefit the development of mitigation strategies against online business credit card fraud. The participants received information in written and verbal communication that this study does not include any financial incentives.

Data Collection Instruments

As the researcher of this study, I was the primary data collection instrument in this qualitative study. I used semistructured interviews to gather the data because semistructured interviews improve the researcher's understanding of the participants' experiences (see DeJonckheere & Vaughn, 2019). Semistructured interviews allow participants to explain their experiences in-depth (Peesker et al., 2019). I engaged in careful planning ahead of the interviews (see McGrath et al., 2019). The interview protocol (Appendix B) served as a guide to keep consistency in the dialog with the participants and improve reliability (Wixted et al., 2018). I familiarized myself with the data recording equipment ahead of the interview (see McGrath et al., 2019). I recorded the interviews using the Zoom provided recording feature. I provided a copy of the

summarized interview to the participants for member checking. Researchers use member checking to present the interpretations from the interview questions to the participants to verify if any information was misinterpreted or left out (Iivari, 2018). During member checking, the participants had the opportunity to make any adjustments to the summary and respond to follow-up questions. Providing the participants with a summary of their interview responses allows the participants the opportunity to review the information and correct any inconsistencies or possible bias (Agnew et al., 2018; Peesker et al., 2019).

I used archival records, interviews, and business investment rating reports to corroborate or extend the data obtained from the interview questions (Appendix A). Secondary data collection instruments such as business documents corroborate evidence collected from other sources (Yin, 2018). I enhanced the reliability and validity of the data collection through member checking follow-up interviews (Appendix C). Researchers use research validity to ensure the robustness of the research study (Yin, 2018).

Data Collection Technique

I researched the professional backgrounds of the participants and their organizations via public records after the participants: (a) consented to participate in the study, (b) understood the purpose of the study, (c) knew the expectations of the interview process, and (d) understood their rights as participants. Understanding the participants' backgrounds ensures the participants will provide rich data that address the study's research question (Van Puyvelde, 2018).

I used audio-recorded online calls to collect the data using a semistructured interview technique that followed the interview protocol (Appendix B). According to Yin (2018), researchers should record participants' interviews to interpret them accurately. The advantages of using the semistructured interview data collection technique include: (a) rich data gathering, (b) the opportunity to ask the participants open-ended questions, and (c) the opportunity for clarification and follow-up questions. Alamri (2019) stated some disadvantages of using the semistructured interview as the data collection technique include (a) the interview, the transcription, and the member checking processes are time-consuming; (b) participants may have trouble in allocating enough time for the full interview, and (c) participants who experience limited time availability might limit the depth of their responses. The interviews lasted for 45 to 60 minutes, with an average interview time of 50 minutes.

I transcribed the audio recordings from the interviews keeping fidelity to what was said and keeping data safe and confidential within 48 hours of each interview. According to McGrath et al. (2019), researchers should transcribe the data as soon as possible after completing the interview to start identifying similarities and differences between the interviewees' experiences. I used member checking to ensure the validity of the research findings (see Brear, 2019). I provided the participants with a summary of the data gathered during the interview to review the material for accuracy or clarification. During the member-checking process, I confirmed or added the data collected during the interview according to the participant's directions. The participants' reviews and transcription correction enhanced research validity (Usman, 2018). I took detailed notes

of my observations during the data collection process based on a framed approach congruent with the conceptional framework and methodological approach (see Phillippi & Lauderdale, 2018). According to Phillippi and Lauderdale (2018), taking notes and observations are essential components of the data collection process.

Data Organization Technique

I assigned a pseudonym for each participant, such as P1, P2, P3, and B1, B2, B3, for the business to keep their identities confidential (see Butler et al., 2019). I also coded the data to remove excess information and identify emerging themes. Coding reduces excess data and highlights the message's core meaning (Clark & Veale, 2018). I organized the data in chronological order in color-coded digital folders and kept all hard copies in a binder tabbed according to the company name. I kept track of the interview participation process in Excel, using Microsoft Word to transcribe each interview audio. I used NVivo to code the data and to identify themes. This study's soft data remains stored on a password-protected portable thumb drive. I saved the secured thumb drive and hard copy data in a secure weatherproof lockbox. According to Yin (2018), researchers are responsible for data storage. Surmiak (2018) noted researchers are responsible for protecting the participant's identity. I stored the electronic data in a password-protected thumb drive and the hard copies in a locked cabinet. After 5 years, I will delete and shred all the gathered data.

Data Analysis

Researchers use triangulation to test the study's validity by observing and analyzing the subject matter from multiple sources of information (Yin, 2018). According

to Noble and Heale (2019), triangulation is a valuable tool to check for biases and inconsistencies. Researchers can triangulate data in several ways, such as using multiple methodologies, multiple theories, multiple data analysis techniques, multiple data sources, or multiple investigators (Natow, 2019). For this multiple case study, I selected a multiple data source triangulation. I gathered and compared data from open-ended interviews, member checking, archival records, and business investment rating reports to achieve data source triangulation. Natow (2019) stated that data triangulation is valuable in studies interviewing leaders. Therefore, I selected data triangulation to interview online business leaders. I reached data source triangulation by using multiple data sources to improve reliability and validity, as Moser and Korstjens (2018) described.

I used the five-phase data analysis process described by Yin (2018): (a) collect the data, (b) decompose the data, (c) generate codes and clusters, (d) interpret the data, and (e) generate a conclusion. The raw data used for this multiple case study was organized in chronological order by participant pseudonym in digital and hard copy form. I used NVivo software to store, manage, and filter unstructured data, including progress reports, interview transcriptions, and member checking responses (see Dalkin et al., 2020). NVivo's powerful query tools facilitate thematic analysis (Elliott-Mainwaring, 2021). Qualitative researchers discover and build relationships between data, assign and define themes, and create reports (Phillips & Lu, 2018). I used the coded data to generate data sets related to answering the research question. Driven by the SCP, I critically analyzed reoccurring patterns and concepts and allowed themes to emerge. According to Clark and Veale (2018), researchers should engage in reflective and interpretive thinking through

every step of the research process to accurately evaluate the subject matter. Therefore, I immersed myself in the data and searched for meaning and emerging patterns. I identified and defined the themes to interpret the data and reported the themes' interpretations, including their relationships, by engaging in the thematic analysis as described by Castleberry and Nolen (2018).

Reliability and Validity

Reliability and validity are fundamental instruments used by researchers to demonstrate the rigor and trustworthiness of research (Jordan, 2018). Reliability describes the systematic use of research methods for collecting and analyzing the data of the study (Collingridge & Gantt, 2019). Validity refers to the relevancy of the interpretations from a study's collected data (Vakili & Jahangiri, 2018). Reliability and validity determine the replicability, objectivity, and quality of research (Yin, 2018). Without obtaining reliability and validity, researchers may reach inaccurate or unreliable research findings and conclusions.

Reliability

My strategy for obtaining reliability was consistency and carefulness in the research practice's application and documentation, as Yin (2018) described. Meticulous craftsmanship and attention to detail help legitimate the results from a study (Collingridge & Gantt, 2019). I used purposive sampling to ensure the participants could provide information that responds to the research question. According to FitzPatrick (2019), researchers should recruit participants who know the research topic. I used some

instruments and processes such as interview protocol, member checking, and data source triangulation to ensure the study results were dependable to obtain reliability.

The interview protocol (Appendix B) served as my guide to ask the participants all listed interview questions in the same order. An interview protocol is a tool used to conduct interviews consistently (Yeong et al., 2018). I was respectful, attentive, empathetic, built up the participant's ego, and did not use overly academic language to build rapport (Duke et al., 2018). Researchers use member checking to enhance dependability (Yin, 2018). I used the member checking (Appendix C) of data to confirm my interpretations of the participants' responses.

Confirmability describes the degree to which research results can be confirmed or corroborated by other researchers (Korstjens & Moser, 2018). To ensure confirmability, I asked probing questions during the interview, completed follow-up member checking, and used data source triangulation by accessing business progress reports and business investment rating reports. Documentation served to reach triangulation and confirmed the data collected from interviews (Siegner et al., 2018). Probing questions and follow-up member checking enhanced the accuracy of the data collection process. I also kept a reflexive journal to note introspections to reduce potential personal bias (see Rettke et al., 2018). Researchers use reflexivity to remain self-aware and analytical about their role in the research process (Tomaszewski et al., 2020). According to Fusch et al. (2018), researchers' enhanced awareness of personal lenses facilitates a more accurate interpretation of the participants' responses.

Data saturation occurs when additional research produces no new data, themes, or codes (FitzPatrick, 2019). I used purposive sampling, data source triangulation, member checking, and recruited participants until no new information emerged to ensure data saturation.

Validity

According to Collingridge and Gantt (2019), researchers can obtain validity by applying an appropriate research method. Therefore, I meticulously adhered to data collection and analysis techniques such as gathering multiple sources of evidence, establishing a chain of evidence, and detailing the process's documentation to enhance the research design's validity. FitzPatrick (2019) recommended that researchers conduct validation procedures throughout the study to address threats to validation during the process. Therefore, I used data source triangulation, member checking, and data saturation to enhance the validity of this study. By using a multiple case study, member checking, and business reports to converge the results, I enhanced the validity and established the credibility of the study.

Credibility refers to collecting research data's accuracy and depicting the participants' experiences in the research findings (Forero et al., 2018). To obtain credibility, I utilized member checking (Appendix C) and data source triangulation, as described by Korstjens and Moser (2018). I did member checking to verify that the data interpretations obtained from the interviews were accurate (see McGrath et al., 2019). I analyzed the data reports, the interpretations from the interviews, and member checking information to achieve data source triangulation.

Transferability describes the degree to which a qualitative research study can be applied to other settings by other researchers and gets enhanced by a detailed and exhaustive description of the process (Korstjens & Moser, 2018). Therefore, I provided as much detail about the study process and the participants as possible for other researchers to determine this study's applicability to different settings. In addition, I used purposive sampling to select participants who answered the research question.

Transition and Summary

In Section 2, I discussed the description of my role as the researcher, the participants, and the justification for the research method and design. I also presented population and sampling, ethical research, and data collection instruments. I explained the data collection technique, data organization techniques, data analysis, and reliability and validity. In Section 3, I discuss the study's findings, the application to professional practice, the implications for social change, recommendations for action, recommendations for further research, a reflection on my experience within the DBA Doctoral Study process, and the conclusion of this study.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the strategies that some online business leaders use to mitigate the loss of revenue caused by credit card fraud. In this section, I present the findings of this study and the themes that emerged from this research. The data obtained for this research resulted from interview data, a review of archival records and business investment rating reports, and an exhaustive literature review. The findings from this research showed four major themes: (a) data management, analysis, and monitoring, (b) internal stakeholders, (c) customer experience, and (d) partnership with online security tool service provider(s) for strategies used by the participants to mitigate online credit card fraud. The two most prominent themes that emerged from all participants' responses were data management, analysis and monitoring; and internal stakeholders. The participants indicated proactive and retroactive strategies were necessary components for successful fraud mitigation strategies. The results of this research study support Clarke's (1980) SCP. This study's resulting themes were related to the obtained data and the literature review, concentrating on the SCP theory framework.

Presentation of the Findings

This qualitative research study's overarching question was: What successful strategies have online business leaders used to mitigate revenue loss from online credit card fraud? To collect data, I conducted semistructured interviews with five online business leaders consisting of five main open-ended questions and a few follow-up

questions. In addition, I used member checking, archival records, and business investment rating reports from Moody's Investors Service, Inc (2021) to coordinate data source triangulation.

The participants in this qualitative multiple case study were: (a) online business leaders of an organization with 500 employees or more; (b) experienced in implementing successful online credit card fraud solutions; and (c) located in the Southwest region of the United States. Table 1 shows the participants' demographics.

Table 1

Participants' Demographic Information

Online business leader	Number of employees	Years of experience	Location
Participant 1	+10,000	16	Arizona
Participant 2	+10,000	15	Texas
Participant 3	+500	15	Texas
Participant 4	+10,000	17	Arizona
Participant 5	5,000	5	Arizona

I identified the main factors contributing to successful online fraud mitigation strategies from the gathered data and thematic analysis. The four major themes that emerged were (a) data management, analysis, and monitoring, (b) internal stakeholders, (c) customer experience, and (d) partnership with online security tool service provider(s). In this segment, I provide information about the emergent themes and excerpts from the interview responses supporting the themes. Table 2 shows the frequency of participants' responses contribution concerning the themes. Figure 1 illustrates the frequency of responses from all participants related to the four emerged themes from hierarchized responses based on word frequency.

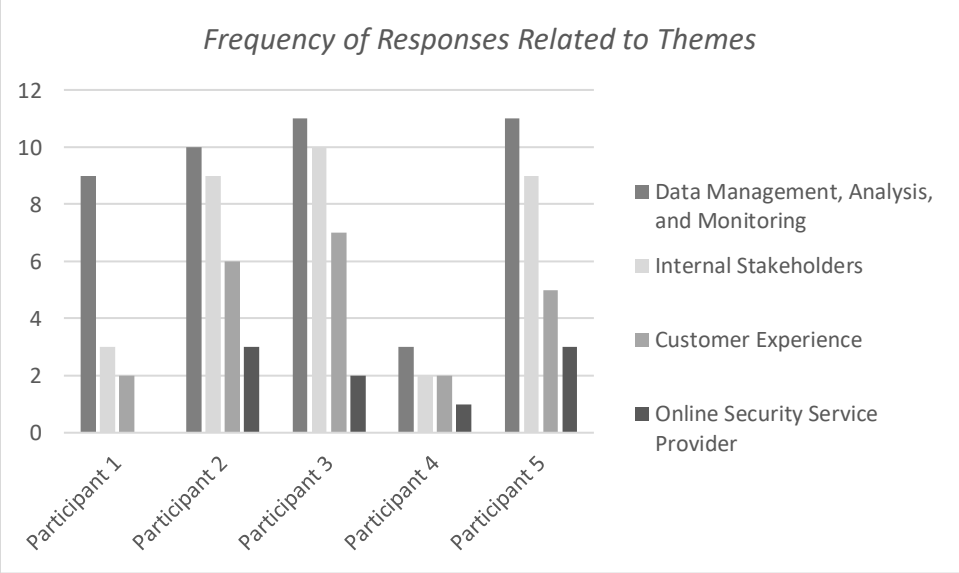
Table 2

Frequency of Responses Related to Themes

Online business leader	Data management, analysis, and monitoring	Internal stakeholders	Customer experience	Online security Service provider
Participant 1	9	3	2	0
Participant 2	10	9	6	3
Participant 3	11	10	7	2
Participant 4	3	2	2	1
Participant 5	11	9	5	3

Figure 1

Frequency of Responses Related to Themes



Theme 1: Data Management, Analysis, and Monitoring

The first theme that emerged from the data collection process was the importance of data management, analysis, and monitoring to fraud mitigation strategy. The results from the data analysis and NVIVO queries demonstrated that the participants rely on data

management, analysis, and monitoring aptitude and agility as of utmost importance to mitigate fraudulent charges. The data-based fraud prevention system includes receiving data related to the transaction, analyzing the transaction's attributes to calculate a score, comparing the score to threshold values, and resolving the case as a valid charge or red-flagging for further scrutiny.

All five participants described data analysis, management, and monitoring as a primary fraud-fighting strategy to mitigate online credit card fraud. P1, P2, P3, P4, and P5 discussed the idea they use data as a fraud authentication tool to confirm the validity of transactions. P1 detailed, "I leveraged the information separately and together, the data knowingly provided by a consumer in an online billing form when transacting, such as the billing address and the data collected unknowingly from the user, such as the IP address." P2 explained

> Strategies that led to reducing fraud are all based on three key factors. The first key factor is rule-based data scoring which is where all transactions were fed into the rule engine, which creates a risk score based on several predetermined criteria. The second key factor is a negative database. The negative database was built over time, included information about known prior fraudulent transactions, and created a high-risk score for future transactions. The third key factor is a positive database which consists of data from known good customers identified over time. Transactions could score themselves out of the queue to lessen the total number of transactions to review.

P5 corroborated, “we have an internal database which we use to compare information inputted on the form online being submitted.” P3 said, “you need to build that positive database before you can even start with pursuing a negative database or knowing who the fosters are or why transactions are not getting through.” P4 attested, “we utilized key factors such as email address used for online purchase to validate the transactions.” All five participants affirmed that building and maintaining an agile and intuitive database process, analysis, and monitoring system is vital to detect fraudulent transactions, separate actual fraud from false triggers, and reduce the number of transactions requiring manual review. Table 3 shows the frequency of participants’ responses related to data management, analysis, and monitoring and the percentage of each participant’s contribution to the theme. Figure 2 illustrates the frequency of responses related to the data management, analysis, and monitoring theme.

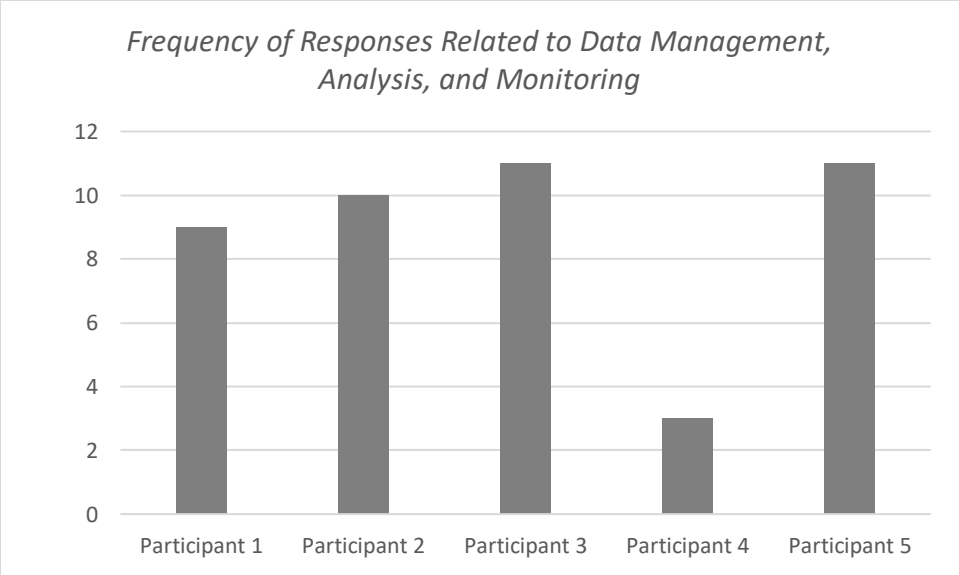
Table 3

Frequency of Responses Related to Data Management, Analysis, and Monitoring

Online business leader	Frequency	Percentage of responses contributing to the theme
Participant 1	9	20%
Participant 2	10	23%
Participant 3	11	25%
Participant 4	3	7%
Participant 5	11	25%

Figure 2

Frequency of Responses Related to Data Management, Analysis, and Monitoring



Connection to the Conceptual Framework

In alignment with Clarke's (1983) SCP framework, the five participants' responses evidenced fraud is a crime of opportunity. Investigators use the SCP framework to understand how individuals take advantage of opportunities to commit a crime (Freilich et al., 2018). The participants explained fraudsters look for and take advantage of opportunities to commit online credit card fraud. The five participants explained how they used data management, analysis, and monitoring to support proactive and retroactive mitigation strategies to block opportunities for fraud. P5 stated,

> When we found out, there was a big problem, and that had to do with the credit card fraud, one of the initial major things I did was turn on address verification and ensure the verification of the CVV number on the back of the customer's credit card.

P4 stated, “we continue to refine our risk rules to increase the effort required to commit fraud and block opportunities for fraudulent charges.” P5 corroborated

> If measures are not set up correctly, there could be an information leakage during the electronic transaction transmission. That’s how the hackers and the bad guys of the world can have an opportunity to get credit card information and can steal all the customer’s money because everything is linked online.

In further alignment with SCP, the participants demonstrated they used data management, analysis, and monitoring to increase the level of difficulty for fraud, risk of getting caught, and the effort required to commit fraud. P2 said, “if we stay consistent in working transactions and shutting them down before a service is provided, the fraudsters know we are taking protection seriously and move on.” P3 corroborated, “we want to impact the fraudsters. We want to get the fraudsters as unsuccessful as possible, and we want to deter them.”

Connection to the Literature

The findings of this study were consistent with Tripathi et al.’s (2018) research results stating that the best way to identify online card fraud is by monitoring and evaluating transaction habits and creating historical data of the customers’ purchasing patterns. All five participants reported using a positive database, which contains the historical data related to positive purchase and customer verified data, and a negative database holding historical data of confirmed fraud, to validate transactions. P4 explained, “We use a methodology of looking at past online history, spending patterns,

and styles." P1 explained, "negative lists allow for challenging or blocking transactions that contain the same data on previous fraud orders." P2 said,

> When looking at total fraud stopped versus fraud missed, our primary goal is to understand better the missed transaction received, why we didn't catch it, and what changes may be necessary to the risk scoring to catch future similar transactions.

The findings were also consistent with Carcillo et al.'s (2019) findings indicating that successful online credit card fraud strategies should incorporate components of supervised learning algorithms (X. Zhang et al., 2019) and unsupervised learning algorithms (Singh & Jain, 2020). The five participants reported using a combination of algorithms supervision approaches, algorithm learning independently, and algorithm taking users' input to enhance the review process. P1 described, "we used currency amount threshold, negative lists, device intelligence strategies, geo-location strategies, device language, and behavior analytics." P4 stated, "We look at past online history, spending patterns, and style to create a risk score based upon the criteria." The red-flagged transactions undergo further scrutiny and validation steps.

Theme 2: Internal Stakeholders

The second theme that emerged from the findings of this study was the importance of the support of the organization's internal stakeholders to fraud mitigation strategies. The results of this study exhibited that the participants depend on the collaboration of internal stakeholders as part of fraud mitigation strategies. Internal stakeholders denote a robust fraud team that is engaged, alert, and astute and the

collaboration of the staff across departments in the organization to support mitigation strategies.

Robust Fraud Team

The responses from the participants demonstrated a robust fraud team is essential to the success of online fraud mitigation strategies. The five participants shared a general agreement of the role of the fraud team in the success of online fraud mitigation strategies. The fraud team aims to stay ahead of the fraudsters by proactive mitigation strategies. P3 stated,

> You got to have the folks who can pivot. A fraud team can pin it and move and be flexible and go from one job to the other. Be ready at the end of the day or end of the week to do something completely different.

The fraud team can identify inconsistencies, uncover evidence, dismantle elaborate fraud schemes, and share their insights with leadership to improve the efficacy of mitigation strategies. P3 explained,

> Managers and directors they're not in the data all the time. The managers and directors are trying to create the vision, but if they're not, you know, getting insight from the fraud team who is engaging with customers and with the data with the systems, then there's going to be a disconnect.

The fraud team verifies and validates transactional information unresolved by the scoring rules. The fraud team manually reviews unresolved transactions to reach case resolutions, classify the data for future analysis, and identify loopholes in the scoring rules. P1 said,

> Out of 100 orders flagged for manual review, 50 are canceled for fraud, which would indicate a 50% fraud cancel rate and would show the fraud strategies are effective. If the fraud cancel rate is 3%, this means the fraud rules are capturing too many legit transactions, and scoring rules need to be tuned.

Three participants shared that the fraud team can also effectively analyze and respond to chargebacks. P2 expressed,

> The fraud team compares the transactions we successfully worked on that resulted in providing the service to transactions that ended up being a chargeback. Our main goal is to understand better what risk score the missed transaction received. Why didn't we catch it? And what changes may be necessary to the risk scoring to catch future-like transactions?

P5 indicated,

> We revamped how the chargebacks from the credit card properties were processed. We developed a routine and understanding of how the fraud team responded to chargeback requests because we were getting hit heavily with fraud.

P3 explained, "you should have robust a team that knows there are certain data elements that are critical for working chargebacks." A robust fraud must learn from the past and anticipate the future to adapt the direction of a strategy or initiative effectively and confidently. Figure 3 illustrates the frequency of responses related to the robust fraud theme. Table 4 shows the frequency of participants' responses related to the robust fraud team theme and the percentage of participants' contribution to the theme.

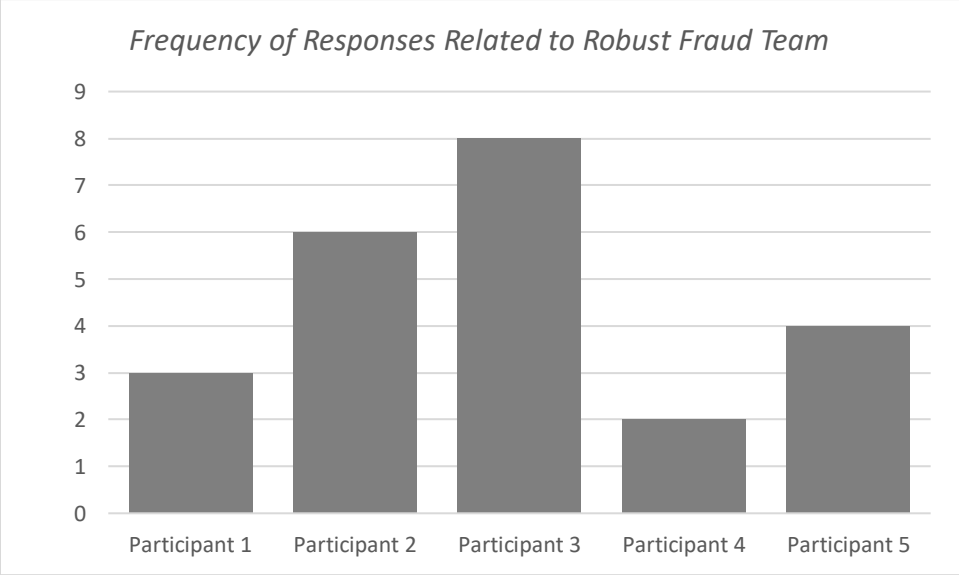
Table 4

Frequency of Responses Related to Robust Fraud Team

Online business leader	Frequency	Percentage of contribution to the theme
Participant 1	3	13%
Participant 2	6	26%
Participant 3	8	35%
Participant 4	2	9%
Participant 5	4	17%

Figure 3

Frequency of Responses Related to Fraud Team



Connection to the Conceptual Framework

The findings of this study aligned with Clarke's (1985) literature that identifying and restricting conditions that facilitate fraud is indispensable for successful fraud mitigation strategies because opportunistic crime is highly susceptible to their environment. Making the crime scene unattractive should influence individuals to choose

against committing the crime. The five participants indicated the fraud team continuously analyzed their environment to determine and limit opportunities for fraud. P2 shared, "our first strategy once we became aware that online sales would trigger a significant amount of fraud was to build an in-house system to review transactions." P2 expanded,

> We find that if the agents can do queue sorting based on their criteria, to bring much more impactful results than just working the transactions with the highest scores. It does help to have an agent assigned for a particular period to work the highest scored transactions specifically, but then allow the other agents to use their instinct, analytics, etc., to find fraud.

P3 said, "from a strategy perspective, we needed to know two things more than anything. One, the data and two, how our customers behaved. From there, we could know what the issues were." P1 opined, "strategies should always be customized to the organization's data and trends." P4 expanded, "our risk rules significantly enhanced during Covid19 as consumers went to less in-person shopping." The participants' responses demonstrate successful fraud mitigation leaders' strategies ensure the right outcome by assessing the environment and challenging fraudsters' opportunities to commit crimes. Figure 3 illustrates the frequency of responses related to the fraud team theme. Table 4 shows the frequency of participants' responses related to the fraud team theme and the percentage of participants' contribution to the theme.

Connection to the Literature

The findings of this study support Nascimento et al.'s (2019) findings that analyzing the cardholder's information and the cardholder's transaction score helped

mitigate credit card fraud. The five participants described analyzing the cardholder's information and the cardholder's transaction score to verify and validate online transactions. P1 described,

> I like to view fraud strategies from a data perspective. When the decision engine challenges a transaction, a human may manually review it, or the customer may be asked to perform an authentication challenge. For example, one-time passcode to the known phone number on file."

P4 stated, "we use a methodology of looking at past online history, spending patterns and styles." P2 shared, we use analytics along with the fraud scoring system and fraud team for much more impactful results".

The results from this research study support Saia and Carta's (2019) research findings, indicating that business leaders who use reactive and proactive strategies design robust fraud mitigation solutions. Reactive strategies prevent further unauthorized charges (Saia & Carta, 2019). Proactive strategies help identify the customer's information and verify a transaction's validity (Sadgali et al., 2020). The five participants described that they used reactive and proactive strategies to mitigate online credit card fraud, such as the fraud team.

Collaboration Across Departments in the Organization

Three participants' responses indicated that the fraud team relies on collaboration across departments in the organization to strengthen online fraud mitigation strategies. Participants P2, P3, and P5 discussed the common viewpoint that collaboration across

departments assures the companywide staff keeps and follows fraud mitigation protocols. P3 explained,

> I discovered over the years that it's not just your department that's being impacted or that needs to be included as you make strategic decisions. For example, somebody orders a flat-screen TV fraudulently online. You need to make sure you have effective communication between your departments.

When leaders across departments collaborate, they reduce opportunities for successful fraud schemes and fraudsters to gain an advantage. Three participants shared that collaboration across departments is not easy to achieve. P3 stated there are a lot of departments that you must get on the same page, and that's very difficult. How do you get through that? Lots of meetings." P2 said

> We presented our marketing team with the proposal to add extra controls up-front to the purchase process. Some leaders did not want to add any friction to the customer experience, which matters strategy-wise because they did not want to add any extra steps for factor authentication during check out of the transaction impacted our fraud mitigation efforts.

P2 explained, "We worked hard to prioritize this project and built a successful business case to show the dollar amounts of fraud loss, the card brand rules that required us to mitigate risk and buy-in from senior leadership." Three participants shared that online business leaders should communicate with other department leaders to unite against online credit card fraud within their organization. P3 stated, "we had lots of strategic planning meetings with various stakeholders such as risk, compliance, and

operations to get everyone in agreement with the strategy." P5 shared, "when sharing within the company fraud mitigation strategy awareness, money always is the number one thing we use to prove to the other departments that the mitigation strategy efforts and investment were worth it." P5 expanded, "soft skills were beneficial to bridge the gap between teams' views and to get everyone in the organization to collaborate with our fraud mitigation strategies." These participants' experience showed that fraud leaders who received support from other department leaders successfully mitigated online fraud and achieved organizational revenue goals. Table 5 shows the frequency of participants' responses related to the collaboration across departments in the organization theme and the percentage of participants' contribution to the theme. Figure 4 illustrates the frequency of responses related to the collaboration across departments in the organization theme.

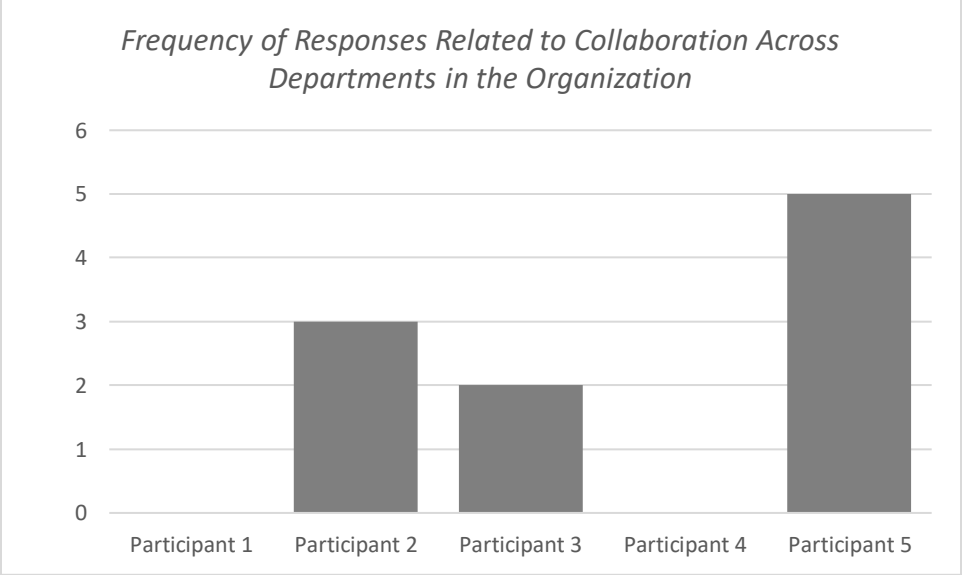
Table 5

Frequency of Responses Related to Collaboration Across Departments in the Organization

Online business leader	Frequency	Percentage of contribution to the theme
Participant 1	0	0%
Participant 2	3	19%
Participant 3	2	25%
Participant 4	0	0%
Participant 5	5	56%

Figure 4

Frequency of Responses Related to Collaboration Across Departments in the Organization



Connection to the Conceptual Framework

The results aligned with Clarke's (1980) specification that SCP is not used to eliminate delinquent tendencies from people or attempts to differentiate between criminal and noncriminal individuals. SCP framework disregards individuals' s sociological, biological, and psychological dispositions to commit the crime. The SCP framework is an evidence-based scientific approach to resolve challenges in the immediate conditions where criminal activity is prone to occur (Mihinjac & Saville, 2019). Three participants indicated mitigation strategies' are not designed to eliminate delinquent tendencies or differentiate between criminals and noncriminal individuals. P5 stated, "we're trying to stop the bad guys, but we are not necessarily trying to find them and punish them." P3 corroborated, "as for fraudsters, we want to stop them as quickly as we possibly can."

Online business leaders support legal authorities with investigations to capture fraudsters, but business mitigation strategies do not correct or identify criminal behavior. Business mitigation strategies are focused on preventing or limiting opportunities for fraud. P4 shared, “unfortunately, fraud doesn’t go away. People love to play games. They love to get things for free, and that is, you know, human nature. Unfortunately, some folks take it a bit too far.” The participants’ responses show that the primary focus of online fraud mitigation strategies is fraud detection and prevention.

Connection to the Literature

The results from this research support Richardson’s (2020) conclusions that businesses with robust online fraud solutions experience fewer losses due to cybercrime. The five participants demonstrated implemented robust fraud mitigation strategies that resulted in a reduction of revenue losses. P5 stated, Within the first few months of putting the extra security stuff and fraud prevention in place, we had already more than doubled the previous revenue ever. And then, we just kept doubling and doubling. P4 stated, “we have taken our loss rate to the best and lowest in the industry with profitability and having continued and improved customer experience.” P3 said, “when I think about mitigation strategies, we had some wins and some losses, but overall, we’re successful.” The findings of this study demonstrated examples of robust mitigation strategies that protected business revenue, safeguarded data, blocked opportunities for fraud, monitored trends, bridged gaps between departments, and educated customers about fraud and ways to protect themselves, their accounts, and their identity.

Theme 3: Customer Experience

The five participants confirmed they considered their customers' purchasing experience to apply fraud mitigation strategies. The participants expressed they designed mitigation strategies that limited adding hurdles to customers during the transaction verification process. P3 shared, "This method was more cautionary than anything because we didn't want to upset customers." P2 stated, "sometimes you find more value for your business in appeasing the good customers versus losing them or steering the fraudsters." P1 stated,

> Determining the difference in data patterns in fraud versus legit orders allows the fraud strategist to write rules to capture as many suspected frauds as possible while capturing the least number of good orders to minimize customer disruptions.

P4 stated, "our goal was reducing customer disruptions while minimizing fraud losses." P5 detailed, "you must find that balance between security controls and customer service." Three participants expressed that emphasis on pleasant customers' purchasing experience provoked friction between leaders from different departments. Some leaders were reluctant to cause inconveniences to the customers' purchasing experience. P3 shared, strategies and security tools go hand in hand together. Some businesses have lowered their fraud tremendously using pre-authorization methods, but they've also upset a lot of customers, so again, there's that balance to maintain."

P5 discussed,

> There is a significant concern that customers give up if you add too many hurdles to the purchasing experience. We want to keep the accounts and purchases secure. Still, we don't want to stress the customers too much into cart abandonment.

P2 corroborated,

> Some leaders did not want to add any friction to the customer experience. They didn't want to add any extra steps to factor authentication. We had challenges within the company to be able to do it. We adapted to make it be something that would work for the entire organization.

P5 shared, "the goal of eCommerce, marketing, and web, mobile, and app teams is to reduce friction and make the best customer experience, and some leaders were against adding one extra step." Online business leadership should set up mitigation strategies that compromise a robust verification process and pleasant customer experience. The five participants of this study showed a strong validation system could co-exist with an enjoyable customer purchasing experience. P4 said, "we have been extremely successful over the last 18 months with record lows in fraud losses. This success came at a small cost to customer satisfaction."

Two of the participants expressed interactions between the fraud team and customers for verification purposes resulted in some customers providing feedback about their customer experience. Participants P3 and P5 indicated their team viewed customers' feedback on fraud intervention techniques as an indicator of the success of their mitigation strategies. P5 stated, "I see an indicator of success the incidental stories that come in from customers appreciating us for helping them protect their credit card account

and account information." P3 said, "we appreciate unwritten customer awards, and sometimes they are written, which is even better. Even just the pat on the back from the customer just saying, thank you. I think of those as in terms of success factors." The participants' responses were evidence that delivering good customers is vital for businesses. It also shows that some business leaders struggle to identify the right balance between good customer service and online fraud mitigation strategies. Table 6 shows the frequency of participants' responses related to customer experience and the percentage of participants' contribution to the theme. Figure 5 illustrates the frequency of the participants' responses related to the customer experience theme.

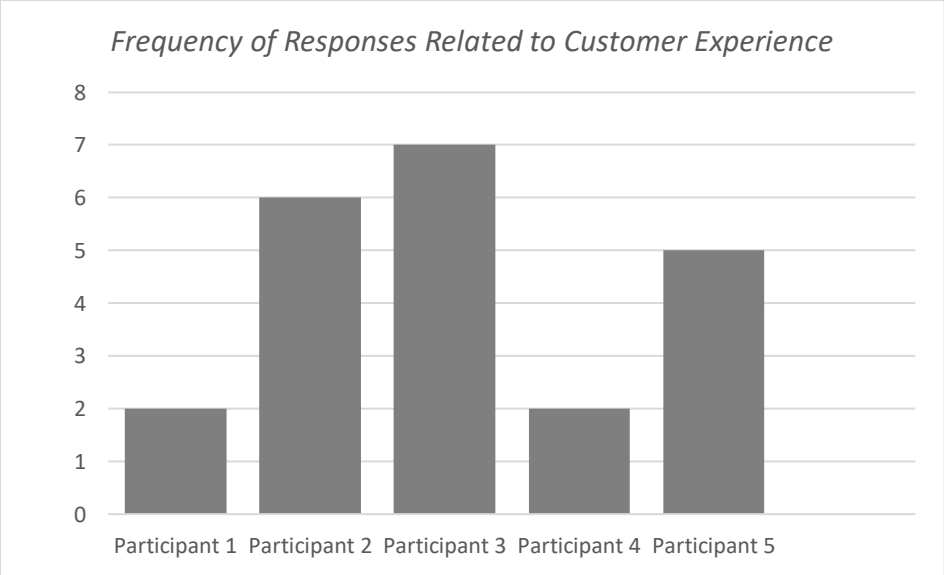
Table 6

Frequency of Responses Related to Customer Experience

Online business leader	Frequency	Percentage of contribution to the theme
Participant 1	2	9%
Participant 2	6	27%
Participant 3	7	32%
Participant 4	2	9%
Participant 5	5	23%

Figure 5

Frequency of Responses Related to Customer Experience



Connection to the Conceptual Framework

The findings of this study aligned with Clarke's (1980) specification that a determined individual could employ countermeasures outside the SCP's strategy scope. Online credit card fraudsters use various methods of operations to commit fraud, some of which are outside the parameters of the fraud team's control, such as hacking customers' accounts and changing customers' account information to make fraudulent charges. P5 described an experience denoting this example,

> We had a particular type of fraud that we identified and corrected. It involved the security of the members' account information. We set up communication alerts for updates on customer information on our database, and we were able to help the members be proactive and protect their data. We also helped customers with protecting their credit card information.

P3 said,

> You want to make sure your technologies are not just looking at your company or just your industry, but across all channels and all industries. If somebody is trying to defraud you with a VISA, in that case, the next time, they might try to defraud your business with a MasterCard or people with some similar data or a similar device used on a different business before yours. Therefore, you want your business to be part of a network that goes across multiple avenues.

P2 shared,

> The fraudsters are a step ahead on things they have seen other businesses do, so when they see we are implementing a new product or service, fraudsters can anticipate what we might not fully understand and take advantage of it.

The participants' responses indicate that fraudsters employ various sophisticated ways and methods to commit fraud and the current scattered online fraud mitigation system has exploitable opportunities for crime. Online fraud mitigation initiatives should engage all parties involved.

Connection to the Literature

This study also aligned with Tilley's (2018) findings that the cost of fraud mitigation strategies influences some business leaders' decisions about implementing fraud mitigation strategies. According to Clarke (1980), some business leaders consider the expense of fraud solutions is not worth the cost. Two participants shared the cost to implement fraud mitigation strategies was an obstacle they overcame. P3 shared we want to send our payment technology resources to generate revenue. Fraud mitigation typically

is not revenue-generating, that's revenue protecting, but it's not necessarily generating revenue. That's the internal struggle, the cost factors.

P5 corroborated,

> We must balance the initial cost of getting things like profile change notifications and changing AVS/CVV rules in place with the results. Does the initial cost of the technical project team's work and the time it takes to get in place worth the long-term benefits to customers and the company? Does the cost of getting anything to market make sense versus continuing to do nothing?"

The participants' responses were evidence some business leaders are hesitant to invest in the expense of fraud mitigation solutions due to ambiguity about finding the optimal balance between the cost of fraud due to losses and the cost of mitigating fraud.

Theme 4: Online Security Service Provider

Four participants discussed the value of partnering with an online security service provider(s) to support online card fraud mitigation strategies. Four participants reported they hired at least one online security tool provider. P2 said, "just as our chargeback rate was hitting an all-time high, we began to meet with the very few fraud prevention vendors in the market. We ended up with a startup." P4 said, "part of our strategy is the use of technology tools that become available to assist with virtual identification and authentication, such as Intellicheck and NotaryCam." P3 stated, "some security tools we used are: Accertify, Ethoca, and Emailage." P5 explained,

> Security tools services could run the verification before the credit card companies and see if any of that information or customers' online activity, like their email

> address, profile, etc., has been included in some other breach. They also monitor the points transactions through their national and international access to networks and loyalty programs.

P5 expanded, "I want to purchase the most secure online engine in the entire industry because that's what I would like as a customer." The responses from the participants demonstrate mitigating online card fraud strengthens with the support from an online security service provider(s) that aligns with the business model and industry. Table 7 shows the frequency of participants' responses related to the online security service provider and the percentage of participants' contribution to the theme. Figure 6 illustrates the frequency of responses related to the online security service provider theme.

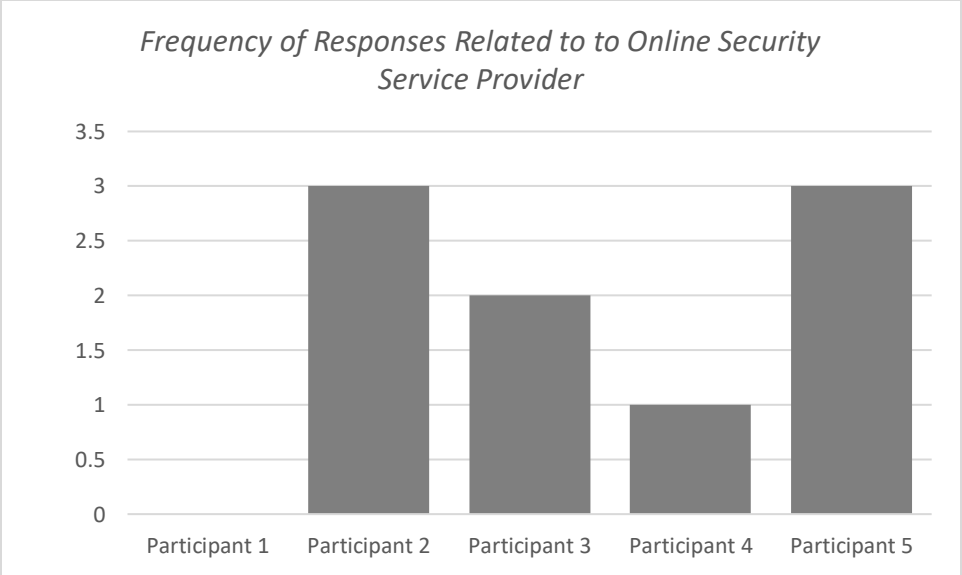
Table 7

Frequency of Responses Related to Online Security Service Provider

Online business leader	Frequency	Percentage of contribution to the theme
Participant 1	0	0
Participant 2	3	33.3%
Participant 3	2	22.2%
Participant 4	1	11.1%
Participant 5	3	33.4%

Figure 6

Responses Related to Online Security Service Provider



Connection to the Conceptual Framework

The results of this research support Cornish and Clarke's (2003) assertion that a successful SCP implementation depends on surveillance and control over the area prone to criminal activity. Leaders cannot mitigate online fraud successfully without adequate information and domain over the area prone to fraud. Four of the five participants share the value of adding a security tool service provider to mitigation strategies. P4, shared, we use the assistance of virtual identification and authentication tools." P5 stated,

> Partnership with a proper online security tool is excellent because it has a tool that is bigger than what our business database could hold. The provider could find and stop a fraudulent transaction before it happens much faster than we would ever do.

P3 explained, “the technological support you side with, they’re going to stay with what’s current in the marketplace.” The participants’ responses show that partnership with an online security service provider(s) augment fraud mitigation strategies’ data volume and surveillance scope.

Connection to the Literature

The research findings aligned with Montague’s (2010) recommendation that business leaders should assess their business risk level and financial resources to decide which security service provider they should hire. Various fraud solution providers can assist with different business fraud mitigation challenges. Business leaders can select a provider according to their risks and challenges of fraud, industry, business model, and financial resources. P2 stated, “As our chargeback rate was hitting an all-time high, we began to meet with fraud prevention vendors in the market. There were two main vendors at the time that understood the intricacies of our industry sales model.” P2 expanded, “partnership with an appropriate security service provider was valuable.” P5 shared some of the questions used as guidance to determine the appropriate service provider for their business. P5 said,

> Do current vendors have what we need to make the enhancements we need? Should we put that effort into a different solution that’s more future-proof (FIDO2 standard) even if it costs double and will take 6 months longer? Does the cost and benefits of taking a two-phased approach make more sense? Do we implement the current but potentially less effective solution first and then enhance it later?

P3 said, “hiring an online security service provider was a significant change because it was just a smarter tool. It was more intuitive of what we were trying to achieve.” The data collected from the interviews demonstrate that hiring online security service provider(s) that matches the organization’s needs is vital for successful fraud mitigation strategies.

Word clouds provide a visual representation summarizing written content based on text frequency (Felix et al., 2018). I used NVivo software to generate a word cloud merging the participants’ responses from the interview questions and member checking highlighting the most frequent words used (see Figure 7). The font sizes in the word cloud denote word frequency. Figure 7 illustrates a word cloud of all participants’ responses to the interview questions and member checking.

Figure 7

Word Cloud of Frequency Query Results of Interview Questions

Applications to Professional Practice

The rapid growth in cybercrimes is a primary concern for online businesses in the 21st century (Ali et al., 2019). The protection of the online transactional environment is a fundamental component of a sustainable global payment system (Kolodiziev & Kotsiuba, 2019). The findings of this study indicated some online business leaders in the Southwest of the United States developed successful strategies to mitigate revenue loss from credit card fraud. All participants achieved significant fraud mitigation levels because of their approach to solving this business problem. P5 shared they won multiple yearly awards due to their fraud mitigation strategies. Online business leaders can apply the themes from this study's findings to set up effective fraud solutions and mitigate the loss of revenue from fraud.

The first theme that emerged from the findings was data management, analysis, and monitoring. The responses from the participants emphasized the value of data management agility. The participants declared using a positive and a negative database to collect historical data and validate transactions authenticity. The participants indicated that data management, analysis, and monitoring help reduce the time devoted to the validation process. Online business leaders can apply this recommendation to leverage their data. The second theme that emerged was internal stakeholders. The responses from the participants reflected they regard a robust fraud team as a vital component of fraud mitigation strategies. The online business leaders interviewed for the study stated a robust fraud team was critical for supporting the initiatives, handling processes, and providing insight contributing to the refinement and strengthening of mitigation strategies. Business

leaders can apply these proven techniques to ensure appropriate procedures, gather relevant feedback, and safeguard the strategy. The responses from the participants evidenced the importance of getting all departments within the organization aligned with fraud mitigation strategies. Online business leaders can strengthen their fraud mitigation strategies by recruiting collaboration across departments in the organization.

The third theme developed from the findings was customer purchasing experience in designing fraud mitigation strategies. The participants' responses demonstrated they created mitigation initiatives that do not disrupt legitimate charges and minimize inconveniencing cardholders. Online business leaders should consider customer experience in designing fraud mitigation strategies. Using techniques such as account information update alerts and customer engagement could strengthen mitigation strategies while assuring a pleasant customer experience. The fourth theme that emerged from the findings of this study was hiring support from online security tool provider(s). Four participants described they hired online security tool provider(s) to support mitigation strategies. Business leaders should assess their business risk level and financial resources to decide if they should employ provider(s). If so, which service provider(s) are needed to address their fraud mitigation challenges.

Online business leaders can apply the emerged themes for setting up robust fraud mitigation strategies while providing a positive customer purchasing experience. The participants' responses demonstrated that they successfully mitigated revenue loss due to credit card fraud while delivering a positive customer experience using these strategies. If

business leaders focus on developing a system that integrates the listed components, they can effectively set up and maintain online credit card fraud solutions.

Implications for Social Change

The findings from this research study could potentially achieve positive social change by illustrating examples of successful mitigation strategies used by online business leaders, which could help retain or gain consumer confidence in online shopping and stimulate communities' economic growth. This research study's findings could also contribute to positive social change by reducing consumers' collateral damage of credit card fraud such as identity theft, phishing, scamming, monetary loss, and mental anguish. Additionally, businesses could allocate resources to initiate or support community programs to teach and empower individuals to control their personal and financial information during online transactions. Such practices encourage collaboration between individuals, businesses, and stakeholders could catalyze communities' safety. Legal authorities could also utilize the findings of this study to develop initiatives, programs, and policies that support online fraud mitigation strategies, consumer empowerment, and data protection.

Recommendations for Action

The results from this research study are relevant to online business leaders because it provides practical ways to set up procedures and practices to mitigate online credit card fraud in their organization and support the integrity of online commerce. Based on the results of this study, below I list my recommendations for action to provide

insight related to successful strategies used by the participants to mitigate online credit card fraud.

Recommendation 1: Data Protection

Online business leaders should protect cardholders' information and business data. As more consumers have gone to less in-person shopping, an influx of online payment transactions has raised the volume of data online, requiring robust and reliable privacy-protection technologies. Online business leaders should develop system security strategies that ensure cardholders' and business' data protection.

Recommendation 2: Fraud Prevention Staff Training

Business leaders interested in online fraud mitigation should identify and correct barriers to collaboration across departments in an organization. Some participants seemed to miss opportunities to strengthen their mitigation strategies by internal collaboration between departments. Online business leaders should provide yearly or bi-yearly training programs for the company's staff, highlighting ways to contribute and support online fraud mitigation strategies.

Recommendation 3: Business Coalition- Collaboration Across Industries

Online business leaders should build a coalition of businesses across industries to widen the scope of surveillance and limit opportunities for online fraud. The lack of collaboration across business industries opens opportunities for fraudsters to commit online credit card fraud. Business leaders should create an online businesses alliance to reduce opportunities for online fraud.

Recommendation 4: Revenue Mitigation Potential Revenue Generator

Online business leaders should consider adopting revenue mitigation strategies as a potential revenue generator. Business leaders should evaluate their transaction process and identify revenue opportunities concurrent with fraud mitigation strategies.

Recommendation 5: Customer Engagement

Online business leaders should engage customers in fraud mitigation strategies by sharing information about fraud trends, educating customers about ways to protect their data online, and sending customers fraud alerts. Business leaders should incentivize customers to protect their online personal and payment data and report fraud. Customer engagement can support fraud mitigation strategies and improve the customer service experience.

Disseminating the Results

I plan to share the findings of this study in peer-reviewed scholarly journals, including business and research journals. I also plan to post on social media channels, such as LinkedIn publishing, Google Scholar, ScienceDirect, and international business sites. I intend to present the findings at webinars and YouTube.

Recommendations for Further Research

The purpose of this qualitative research study was to explore successful strategies online business leaders used to mitigate revenue loss due to credit card fraud. The findings of this study provide examples of strategies used by online business leaders' to mitigate the loss of revenue due to credit card fraud. A recommendation for further research includes exploring this study's overarching question from online security service

provider leaders' perspectives. Another recommendation for further research is to explore the relationship between online fraud mitigation strategies and customer experience.

The first limitation of this study is that the number of participants represents a relatively small sample size. Future research could explore replication of this study using a larger sample size. An opportunity for future research could examine the overarching question for this study with participants at other geographical locations. Another limitation of this research study is that the data collected may have not adequately represented the experiences of all online business leaders who have implemented effective online mitigation strategies against credit card fraud. Future research could consider evaluating online fraud business leaders' leadership style(s).

Reflections

During this challenging and rewarding DBA journey to change my career path and become a doctoral university chair, I grew academically and in my personal life. I am grateful for this transformational experience. I had the opportunity to learn under and alongside excellent faculty members and colleagues who challenged me to research the topic of this study from lateral thinking. I also appreciate the remarkable group of participants who joined this research to support the body of business industry knowledge and my research study. These participants were prominent leaders of an organization with hectic schedules but arranged time to participate in this research study. It was an honor to have met with each participant, and I am grateful for their contribution.

Although I held a role as part of an online fraud team for a large organization, I did not have preconceived ideas about the results of this study. I did have knowledge

related to the subject, such as the value of data management technology and the use of fraud security service providers. I was unaware of the details considered by leadership when planning mitigation strategies. In addition, I terminated my role in revenue protection 3 years ago to focus on researching this topic objectively. I kept an open and flexible mind to welcome the results of this research. To limit my personal bias, I developed and adopted an interview protocol (Appendix B), asked the interview questions (Appendix A) in the same order to all the participants, and kept a reflexive journal to note introspections, as Rettke et al. (2018) described. The findings of this research study were genuinely informative to me.

In my DBA journey, I initiated and facilitated a support group for DBA Walden University's students at the dissertation level. I held biweekly conference calls to discuss each member's challenges and provide feedback on our work. We also discussed ideas to overcome doctoral student-related challenges. We celebrated each other triumphs too. Monthly, I hosted a guest speaker graduate from the Walden DBA program to share their DBA journey experience, provide insight, and respond to questions from the group. Leading this group for over a year was a rewarding experience. I want to become a doctoral chair member to guide and support other doctoral students. I also want to open my practice to help business leaders and customers protect themselves from online fraud.

Conclusion

Online shopping is an increasing prospect for continued global economic stimulation. Many customers are willing to participate in online shopping when they trust the payment system and have a pleasant customer service experience. The rise of online

credit card fraud jeopardizes the security and reliability of e-commerce and customers' trust in online shopping. Business leaders play an essential role in protecting customers' data and securing the online payment system. Informing business leaders about strategies to mitigate revenue loss due to online credit card fraud could help strengthen the payment system and gain or retain customers' confidence in online shopping.

The purpose of this research study was to provide information that could support online business leaders in identifying potential fraud threats and implementing fraud mitigation strategies that help decrease fraudulent activity. The findings of this research demonstrate some examples of critical components for successful and effective mitigation strategies. The themes developed in this research study indicate that online business leaders that successfully mitigated online credit card fraud used (a) data management, analysis, and monitoring, (b) internal stakeholders, (c) customer experience, and (d) partnership with online security tools service provider(s). The emerged themes aligned with SCP conceptual framework and the literature review. Online business leaders are encouraged to apply these strategies for effective fraud solutions.

References

Abdulai, M. A. (2020). examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology*, *14*(1), 157–174. https://doi.org/10.5281/zenodo.3749468

Agnew, D., Marks, A., Henderson, P., & Woods, C. (2018). Deselection from elite Australian football as the catalyst for a return to sub-elite competitions: When elite players feel there is 'still more to give.' *Qualitative Research in Sport, Exercise and Health*, *10*(1), 117–136. https://doi.org/10.1080/2159676X.2017.1380074

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15. https://doi.org/10.1093/cybsec/tyy006

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Farheen, Z. (2019). Qualitative v/s. Quantitative research: A summarized review. *Journal of Evidence-Based Medicine and Healthcare*, *6*(43), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Northeastern University Press.

Akila, S., & Srinivasulu Reddy, U. (2018). Cost-sensitive risk-induced bayesian conference bagging (RIBIB) for credit card fraud detection. *Journal of*

Computational Science, *27*, 247–254. https://doi.org/10.1016/j.jocs.2018.06.009

Alamri, W. A. (2019). Effectiveness of qualitative research methods: Interviews and diaries. *International Journal of English and Cultural Studies*, *2*(1), 65–70. https://doi.org/10.11114/ijecs.v2i1.4302

Alavi, M., Archibald, M., McMaster, R., Lopez, V., & Cleary, M. (2018). Aligning theory and methodology in mixed methods research: Before design theoretical placement. *International Journal of Social Research Methodology*, *21*(5), 527–540. https://doi.org/10.1080/13645579.2018.1435016

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019, November). Consumer-facing technology fraud: Economics, attack methods, and potential solutions. *Future Generation Computer Systems*, *100*, 408–427. https://doi.org/10.1016/j.future.2019.03.041

Al-Maliki, O., & Al-Assam, H. (2021). Challenge-response mutual authentication protocol for EMV contactless cards. *Computers & Security*, *103*, 1–12. https://doi.org/10.1016/j.cose.2021.102186

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association*, *107*(1), 1–5. https://doi.org/10.5195/jmla.2019.615

Amasiatu, C. V., & Shah, M. H. (2019). The management of first party fraud in e-tailing: A qualitative study. *International Journal of Retail & Distribution Management*, *47*(4), 433–452. https://doi.org/10.1108/ijrdm-07-2017-0142

Ansari, G., Saxena, C., Ahmad, T., & Doja, M. N. (2020). Aspect term extraction using graph-based semi-supervised learning. *Procedia Computer Science*, *167*, 2080–2090. https://doi.org/10.1016/j.procs.2020.03.249

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using Zoom videoconferencing for qualitative data collection: Perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, *18*, 1–8. https://doi.org/10.1177/1609406919874596

Attigeri, G., M M, M. P., Pai, R. M., & Kulkarni, R. (2018). Knowledge base ontology building for fraud detection using topic modeling. *Procedia Computer Science*, *135*, 369–376. https://doi.org/10.1016/j.procs.2018.08.186

Ballena, C. T. (2021). Qualitative research interviewing: Typology of graduate students' interview questions. *Philippine Social Science Journal*, *4*(3), 96–112. https://doi.org/10.52006/main.v4i3.376

Bansal, P., Smith, W. K., & Vaara, E. (2018, August). New ways of seeing through qualitative research. *Academy of Management Journal*, *61*(4), 1189–1195. https://doi.org/10.5465/amj.2018.4004

Bashir, S., Anwar, S., Awan, Z., Qureshi, T. W., & Memon, A. B. (2018). A holistic understanding of the prospects of financial loss to enhance shopper's trust to search, recommend, speak positive, and frequently visit an online shop. *Journal of Retailing and Consumer Services*, *42*, 169–174. https://doi.org/10.1016/j.jretconser.2018.02.004

Baskarada, S., & Koronios, A. (2018). A philosophical discussion of qualitative, quantitative, and mixed methods research in social science. *Qualitative Research Journal*, *18*(1), 2–21. https://doi:10.1108/qrj-d-17-00042

Beccaria, C. (1764). *On Crimes and Punishment*. Bobbs-Merrill.

Becker, H. S. (1963). *Outsiders*. Free Press.

Bentham, J. (1789). *An introduction to the principles of morals and legislation. The collected works of Jeremy Bentham: An introduction to the principles of morals and legislation.* Oxford University Press.

Braithwaite, J. (1989). *Crime, shame, and reintegration*. Cambridge University Press. http://doi.org/10.1017/CBO9780511804618

Brantingham, P. L., & Brantingham, P. J. (1981). *Environmental Criminology*. Sage Publications.

Brantingham, P. L., Brantingham, P. J., & Taylor, W. (2005). Situational crime prevention as a key component in embedded crime prevention. *Canadian Journal of Criminology & Criminal Justice*, *47*(2), 271–292. https://doi.org/10.3138/cjccj.47.2.271

Brear, M. (2019, June). Process and outcomes of a recursive, dialogic member checking approach: A project ethnography. *Qualitative Health Research*, *29*(7), 944–957. https://doi.org/10.1177/1049732318812448

Brimbal, L., Meissner, C. A., Kleinman, S. M., Phillips, E. L., Atkinson, D. J., Dianiska, R. E., Rothweiler, J. N., Oleszkiewicz, S., & Jones, M. S. (2021). Evaluating the benefits of a rapport-based approach to investigative interviews: A training study

with law enforcement investigators. *Law and Human Behavior*, *45*(1), 55–67. https://doi.org/10.1037/lhb0000437

Buetow, S. (2019, January). Apophenia, unconscious bias, and reflexivity in nursing qualitative research. *International Journal of Nursing Studies*, *89*, 8–13. https://doi.org/10.1016/j.ijnurstu.2018.09.013

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social Problems*, *14*(2), 128–147. https://doi.org/10.1525/sp.1966.14.2.03a00020

Butler, A. E., Copnell, B., & Hall, H. (2019). Researching people who are bereaved: Managing risks to participants and researchers. *Nursing Ethics*, *26*(1), 224–234. https://doi.org/10.1177/0969733017695656

Cai, T., Du, L., Xin, Y., & Chang, L. Y. C. (2018). Characteristics of cybercrimes: Evidence from Chinese judgment documents. *Police Practice and Research*, *19*(6), 582–595. https://doi.org/10.1080/15614263.2018.1507895

Capili, B. (2021). Selection of the study participants. *American Journal of Nursing*, *121*(1), 64–67. https://doi.org/10.1097/01.NAJ.0000731688.58731.05

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, *557*, 1–15. https://doi.org/10.1016/j.ins.2019.05.042

Castleberry, A., & Nolen, A. (2018, June). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019

Charki, M. H., Josserand, E., & Boukef, N. (2017, March). The paradoxical effects of legal intervention over unethical information technology use: A rational choice theory perspective. *Journal of Strategic Information Systems*, *26*(1), 58–76. https://doi.org/10.1016/j.jsis.2016.07.001

Chavez, N., & Bichler, G. (2019). Guarding against cyber-trespass and theft: Routine precautions from the hacking community. *International Journal of Cyber Criminology*, *13*(1), 101–116. https://doi.org/10.5281/zenodo.3551489

Chen, C.-M. (Jimmy). (2018). A review and analysis of service level agreements and chargebacks in the retail industry. *International Journal of Logistics Management, 29*(4), 1325–1345. https://doi.org/10.1108/ijlm-09-2016-0205

Chiu, Y.-N., Leclerc, B., Reynald, D. M., & Wortley, R. (2021). Situational crime prevention in sexual offenses against women: Offenders tell us what works and what doesn't. *International Journal of Offender Therapy & Comparative Criminology*, *65*(9) 1055–1076. https://doi.org/10.1177/0306624x20919712

Cho, S., & Lee, J. M. (2018). Explaining physical, verbal, and social bullying among bullies, victims of bullying, and bully-victims: Assessing the integrated approach between social control and lifestyles-routine activities theories. *Children and Youth Services Review*, *91*, 372–382. https://doi.org/10.1016/j.childyouth.2018.06.018

Choi, J., Kruis, N. E., & Choo, K.-S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice*, *37*(2), 406–426. https://doi.org/10.1177/10439862211001627

Clark, K. R., & Veale, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology*, *89*(5), 482CT–485CT. https://www.asrt.org/

Clarke, R. V. G. (1980). "Situational" crime prevention: Theory and practice. *British Journal of Criminology*, *20*(2), 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, R. V. G. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice*, *4*(1983), 225–256. https://doi.org/10.1086/449090

Clarke, R. V. G., & Cornish, D. B. (1985). Crime control in Britain: A review of policy research. *Contemporary Sociology*, *14*(2), 186–187. https://doi.org/10.2307/2070144

Cohen, L. E., & Felson, M. (1979, August). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Collingridge, D. S., & Gantt, E. E. (2019, September 3). Republished: The quality of qualitative research. *American Journal of Medical Quality*, *34*(5), 439–445. https://doi.org/10.1177/1062860619873187

Conlon, C., Timonen, V., Elliott-O'Dare, C., O'Keeffe, S., & Foley, G. (2020). Confused about theoretical sampling? Engaging theoretical sampling in diverse grounded theory Studies. *Qualitative Health Research*, *30*(6), 947–959. https://doi.org/10.1177/1049732319899139

Cook, A., Reynald, D. M., Leclerc, B., & Wortley, R. (2018, November). Learning about situational crime prevention from offenders: Using a script framework to compare the commission of completed and disrupted sexual offenses. *Criminal Justice Review*, *44*(4), 431–451. https://doi.org/10.1177/0734016818812149

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators, and criminal decisions. In M. J. Smith & D. B. Cornish (eds.), *Crime prevention studies*, *16*, 41–96. Criminal Justice Press.

Croix, A., Barrett, A., & Stenfors, T. (2018). How to...do research interviews in different ways. *Clinical Teacher*, *15*(6), 451–456. https://doi.org/10.1111/tct.12953

Cross, C. (2018). Expectations vs. reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2020). "Oh, we can't actually do anything about that": The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice: An International Journal*, *20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Culatta, E., Clay-Warner, J., Boyle, K. M., & Oshri, A. (2020). Sexual revictimization: A routine activity theory explanation. *Journal of Interpersonal Violence*, *35*(15–16), 2800–2824. https://doi.org/10.1177/0886260517704962

Cumyn, A., Ouellet, K., Cote, A.-M., Francoeur, C., & St-Onge, C. (2019, November). Role of researchers in the ethical conduct of research: A discourse analysis from different stakeholder perspectives. *Ethics & Behavior*, *29*(8), 621–636. https://doi.org/10.1080/10508422.2018.1539671

Dalkin, S., Forster, N., Hodgson, P., Lhussier, M., & Carr, S. M. (2020). Using computer assisted qualitative data analysis software (CAQDAS; NVivo) to assist in the complex process of realist theory generation, refinement, and testing. *International Journal of Social Research Methodology*, *24*(1), 123–134. https://doi.org/10.1080/13645579.2020.1803528

Daroch, B., Nagrath, G., & Gupta, A. (2021). A study on factors limiting online shopping behavior of consumers. *Rajagiri Management Journal*, *15*(1), 39–52. https://doi.org/10.1108/RAMJ-07-2020-0038

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigor. *Family Medicine and Community Health*, *7*(2), 1–8. https://doi.org/10.1136/fmch-2018-000057

Domingues, R., Filippone, M., Michiardi, P., & Zouaoui, J. (2018, February). A comparative evaluation of outlier detection algorithms: Experiments and analyses. *Pattern Recognition*, *74*(2), 406–421. https://doi.org/10.1016/j.patcog.2017.09.037

Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. *Procedia Computer Science*, *165*, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

Downing, C. O., Jr., Capriola, N., & Geller, E. S. (2018, October). 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. https://doi.org/10.1080/01608061.2018.1514349

Duke, M. C., Wood, J. M., Bollin, B., Scullin, M., & LaBianca, J. (2018). Development of the rapport scales for investigative interviews and interrogations (RS3i), interviewee version. *Psychology, Public Policy, and Law*, *24*(1), 64–79. https://doi.org/10.1037/law0000147

Elliott-Mainwaring, H. (2021). Exploring using NVivo software to facilitate inductive coding for thematic narrative synthesis. *British Journal of Midwifery*, *29*(11), 628–632. https://doi.org/10.12968/bjom.2021.29.11.628

Erlingsson, C., & Brysiewicz, P. (2018). Orientation among multiple truths: An introduction to qualitative research. *African Journal of Emergency Medicine, 3*, 92–99. https://doi.org/10.1016/j.afjem.2012.04.005

Federal Bureau of Investigation. (2018). *2017 Internet Crime Report.* (Internet Crime Complaint Center). https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Bureau of Investigation. (2019). *2018 Internet Crime Report*. (Internet Crime Complaint Center). https://pdf.ic3.gov/2018_IC3Report.pdf

Federal Bureau of Investigation. (2020). *2019 Internet Crime Report*. (Internet Crime Complaint Center). https://pdf.ic3.gov/2019_IC3Report.pdf

Federal Bureau of Investigation. (2021). *2020 Internet Crime Report.* (Internet Crime Complaint Center). https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Felix, C., Franconeri, S., & Bertini, E. (2018). Taking word clouds apart: An empirical investigation of the design space for keyword summaries. *IEEE Transactions on Visualization and Computer Graphics*, *24*(1), 657–666. https://doi.org/10.1109/tvcg.2017.2746018

Felson, M. (2018, August). Policy levels for situational crime prevention. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 198–201. https://doi.org/10.1177/0002716218787471

Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019, April). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences*, *479*, 448–455. https://doi.org/10.1016/j.ins.2017.12.030

FitzPatrick, B. (2019, February). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, *11*(2), 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Forero, R., Nahidi, S., Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarth, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(120), 1–13. https://doi.org/10.1186/s12913-018-2915-2

Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing*, *99*, 1–11. https://doi.org/10.1016/j.asoc.2020.106883

Freilich, J. D., Chermak, S. M., & Klein, B. R. (2020). Investigating the applicability of situational crime prevention to the public mass violence context. *Criminology & Public Policy*, *19*(1), 271–293. https://doi.org/10.1111/1745-9133.12480

Freilich, J. D., Gruenewald, J., & Mandala, M. (2018, October 12). Situational crime prevention and terrorism: An assessment of 10 years of research. *Criminal Justice Policy Review*, *30*(9), 1283–1311. https://doi.org/10.1177/0887403418805142

Fusch, P., Fusch, G. E., & Ness, L. R. (2018, January). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), 19–32. https://doi.org/10.5590/josc.2018.10.1.02

Gelinas, L., Largent, E. A., Cohen, I. G., Kornetsky, S., Bierer, B. E., & Fernandez Lynch, H. (2018, February). A framework for ethical payment to research participants. *New England Journal of Medicine*, *378*(8), 766–771. https://doi.org/10.1056/NEJMsb1710591

Ghaffari, K., & Lagzian, M. (2018). Exploring users' experiences of using personal cloud storage services: A phenomenological study. *Behavior & Information Technology*, *37*(3), 295–309. https://doi.org/10.1080/0144929X.2018.1435722

Ghazali, O., Yang Leow, C., Qaiser, S., Pattabiraman, N., Vasuthevan, S., Abdusalam, E. M., & M. Barakat, M. (2019). Cloud-based global online marketplaces review on

trust and security. *International Journal of Interactive Mobile Technologies*, *13*(4), 96–116. https://doi.org/10.3991/ijim.v13i04.10523

Giannini, G., Ghemmogne Fossi, L., Mio, C., Caelen, O., Brunie, L., & Damiani, E. (2020, January). Managing a pool of rules for credit card fraud detection by a game theory-based approach. *Future Generation Computer Systems*, *102*(1), 549–561. https://doi.org/10.1016/j.future.2019.08.028

Gibaldi, J., & Siddiqi, B. (2019, September). Retention strategies for keeping participants engaged: A case study of the Parkinson's progression markers initiative. *Applied Clinical Trials*, *28*(9), 20–21. http://www.appliedclinicaltrialsonline.com/

GieBmann, S. (2018, August). Money, credit, and digital payment 1971/2014: From the credit card to Apple pay. *Administration & Society*, *50*(9), 1259–1279. https://doi.org/10.1177/0095399718794169

Goldstein, H. (1979, April). Improving policing: A problem-oriented approach. *Crime and Delinquency*, *25*(2), 236–258. https://doi.org/10.1177/001112877902500207

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLOS ONE*, *15*(5), 1–17. https://doi.org/10.1371/journal.pone.0232076

Gunasegaran, M., Basiruddin, R., Abdul Rasid, S. Z., & Mohd Rizal, A. (2018). The case studies of fraud prevention mechanisms in the Malaysian medium enterprises. *Journal of Financial Crime*, *25*(4), 1024–1038. https://doi.org/10.1108/jfc-05-2017-0034

Guo, Y., Bao, Y., Stuart, B. J., & Le, N. K. (2018, March). To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce. *Information Systems Journal*, *28*(2), 359–383. https://doi.org/10.1111/isj.12144

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683–714. https://doi.org/10.1080/07421222.2018.1451962

Hamilton, A. B., & Finley, E. P. (2020, January). Reprint of: Qualitative methods in implementation research: An introduction. *Psychiatry Research*, *283*(2020), 1–8. https://doi.org/10.1016/j.psychres.2019.112629

Hayward, K. (2007, July). Situational crime prevention and its discontents: Rational choice theory versus the "culture of now." *Social Policy & Administration*. *41*(3), 232–250. https://doi.org/10.1111/j.1467-9515.2007.00550.x

Hayward, K., & Hobbs, D. (2007, June). Beyond the binge in booze Britain: A market-led liminalisation and the spectacle of binge drinking. *British Journal of Sociology*, *58*(3), 437–456. https://doi.org/10.1111/j.1468-4446.2007.00159.x

Hennink, M. M., Kaiser, B. N., & Weber, M. B. (2019, August). What influences saturation? Estimating sample sizes in focus group research. *Qualitative Health Research*, *29*(10), 1483–1496. https://doi.org/10.1177/1049732318821692

Hewitt, A. N., Beauregard, E., Andresen, M. A., & Brantingham, P. L. (2018, July-August). Identifying the nature of risky places for sexual crime: The applicability

of crime pattern and social disorganization theories in a Canadian context. *Journal of Criminal Justice*, *57*(7–8), 35–46. https://doi.org/10.1016/j.jcrimjus.2018.03.003

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/10.1080/0735648x.2019.1691859

Hu, Z., Chiong, R., Pranata, I., Bao, Y., & Lin, Y. (2019). Malicious web domain identification using online credibility and performance data by considering the class imbalance issue. *Industrial Management & Data Systems*, *119*(3), 676–696. https://doi.org/10.1108/imds-02-2018-0072

Hussein, A. S., Khairy, R. S., Najeeb, S. M. M., & ALRikabi, H. T. S. (2021). Credit card fraud detection using fuzzy rough nearest neighbor and sequential minimal optimization with logistic regression. *International Journal of Interactive Mobile Technologies*, *15*(5), 24–42. https://doi.org/10.3991/ijim.v15i05.17173

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People*, *31*(1), 111–133. https://doi.org/10.1108/ITP-07-2016-0168

Jacobs, J. (1961). *The death and life of great American cities*. Vintage Books.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Jeffery, C. (1971). *Crime prevention through environmental design*. Sage Publications.

Jenner, B. M., & Myers, K. C. (2019, March). Intimacy, rapport, and exceptional disclosure: A comparison of in-person and mediated interview contexts. *International Journal of Social Research Methodology: Theory & Practice*, *22*(2), 165–177. https://doi.org/10.1080/13645579.2018.1512694

Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018, October). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. *IEEE Internet of Things Journal*, *5*(5), 3637–3647. https://doi.org/10.1109/jiot.2018.2816007

Jordan, G., Leskovar, R., & Maric, M. (2018). Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija*, *51*(2), 146–155. https://doi.org/10.2478/orga-2018-0007

Jordan, K. (2018, May). Validity, reliability, and the case for participant-centered research: Reflections on a multi-platform social media study. *International Journal of Human–Computer Interaction*, *34*(10), 913–921. https://doi.org/10.1080/10447318.2018.1471570

Junger, M., Wang, V., & Schlomer, M. (2020). Fraud against businesses, both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(1), 1–15. https://doi.org/10.1186/s40163-020-00119-4

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018, June). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, *100*(6), 234–245. https://doi.org/10.1016/j.eswa.2018.01.037

Kalbande, J. (2019, June). Ecommerce transactions: Secure Gateway in payment system. *International Journal of Engineering and Technology*. *6*(6), 421–427. https://www.irjet.net

Kalman, M. (2019). "It requires interest, time, patience and struggle": Novice researchers' perspectives on and experiences of the qualitative research journey. *Qualitative Research in Education*, *8*(3), 341–377. http://doi.org/10.17583/qre.2019.4483

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: The power of reflexivity. *International Journal of Interdisciplinary Educational Studies*, *13*(1), 19–31. https://doi.org/10.18848/2327-011x/cgp/v13i01/19-31

Kegler, M. C., Raskind, I. G., Comeau, D. L., Griffith, D. M., Cooper, H. L. F., & Shelton, R. C. (2019). Study design and use of inquiry frameworks in qualitative research published in health education & behavior. *Health Education & Behavior*, *46*(1), 24–31. https://doi.org/10.1177/1090198118795018

Khattri, V., Nayak, S. K., & Singh, D. K. (2020). Plastic card circumvention an infirmity of authenticity and authorization. *Journal of Financial Crime*, *27*(3), 959–975. https://doi.org/10.1108/jfc-03-2020-0034

Khattri, V., & Singh, D. K. (2019). Implementation of an additional factor for secure authentication in online transactions. *Journal of Organizational Computing & Electronic Commerce*, *29*(4), 258–273. https://doi.org/10.1080/10919392.2019.1633123

Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences*, *9*(19), 1–21. https://doi.org/10.3390/app9194018

Kolodiziev, O. M., & Kotsiuba, O. V. (2019). The payment card fraud: Current realities and prevention measures. *Business Inform*, *3*(494), 315–321. https://doi.org/10.32983/2222-4459-2019-3-315-321

Koraus, A., Dobrovic, J., Polak, J., & Backa, S. (2019). Aspects of the security use of payment card pin code analyzed by the methods of multidimensional statistics. *Entrepreneurship and Sustainability Issues*, *6*(4), 2017–2036. http://doi.org/10.9770/jesi.2019.6.4(33)

Korsell, L. (2018). Regulating organized crime. *Annals of the American Academy of Political and Social Science*, *679*(1), 158–177. https://doi.org/10.1177/0002716218782654

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Kroska, A., Lee, J. D., & Carr, N. T. (2017). Juvenile delinquency and self-sentiments: Exploring a labeling theory proposition. *Social Science Quarterly*, *98*(1), 73–88. https://doi.org/10.1111/ssqu.12307

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, *63*, 113–121. https://doi.org/10.1016/j.drugpo.2018.09.013

Lauer, J. (2020). Plastic surveillance: Payment cards and the history of transactional data, 1888 to present. *Big Data & Society*, *7*(1), 1–14. https://doi.org/10.1177/2053951720907632

Leclerc, B., & Savona, E. U. (2016). *Crime prevention in the 21st-century insightful approaches for crime prevention initiatives*. Springer International Publishing. https://doi.org/10.1007/978-3-319-27793-6_4

Lee, J., Jung, J., Park, P., Chung, S., & Cha, H. (2018, June). Design of a human-centric de-identification framework for utilizing various clinical research data. *Human Centric Computing and Information Sciences*, *8*(1), 1–12. https://doi.org/10.1186/s13673-018-0142-9

Lee, V. (2018). Beyond seeking informed consent: Upholding ethical values within the research proposal. *Canadian Oncology Nursing Journal*, *28*(3), 222–224. http://www.canadianoncologynursingjournal.com/index.php/conj

Levi, M. (2017, February). Assessing the trends, scale, and nature of economic cybercrimes: Overview and issues. *Crime, Law, and Social Change*, *67*(1), 3–20. https://doi.org/10.1007/s10611-016-9645-3

Levitt, H. M., Morrill, Z., Collins, K. M., & Rizo, J. L. (2021). The methodological integrity of critical qualitative research: Principles to support design and research review. *Journal of Counseling Psychology*, *68*(3), 357–370. https://doi.org/10.1037/cou0000523

Li, H., Luo, X., Zhang, J., & Sarathy, R. (2018, April). Self-control, organizational context, and rational choice in internet abuses at work. *Information & Management*, *55*(3), 358–367. https://doi.org/10.1016/j.im.2017.09.002

Li, Y., Deng, S., & Zhang, Y. (2019). Research on the motivation to contribution and influencing factors of university students–A semi-structured interview based on qualitative research. *IOP Conference Series: Materials Science and Engineering*, *563*(5), 1–5. https://doi.org/10.1088/1757-899x/563/5/052095

Lokanan, M. (2018). Theorizing financial crimes as moral actions. *European Accounting Review*, *27*(5), 901–938. https://doi.org/10.1080/09638180.2017.1417144

Lupovici, A. (2019). Toward a securitization theory of deterrence. *International Studies Quarterly*, *63*(1), 177–186. https://doi.org/10.1093/isq/sqy045

Magnat, V. (2018, December). A traveling ethnography of voice in qualitative research. *Cultural Studies/Critical Methodologies*, *18*(6), 430–44. https://doi.org/10.1177/1532708617742407

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*, *7*, 93010–93022. https://doi.org/10.1109/access.2019.2927266

Manlangit, S., Azam, S., Shanmugam, B., & Karim, A. (2019). Novel machine learning approach for analyzing anonymous credit card fraud patterns. *International Journal of Electronic Commerce Studies*, *10*(2), 175–201. https://doi.org/10.7903/ijecs.1732

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1002–1006. https://doi.org/10.1080/0142159X.2018.1497149

Mekterovic, I., Karan, M., Pintar, D., & Brkic, L. (2021). Credit card fraud detection in card-not-present transactions: Where to invest? *Applied Sciences*, *11*(15), 1–20. https://doi.org/10.3390/app11156766

Menting, B. (2017, October). Awareness × opportunity: Testing interactions between activity nodes and criminal opportunity in predicting crime location choice. *British Journal of Criminology*, *58*(5), 1171–1192. https://doi.org/10.1093/bjc/azx049

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356–1371. https://doi.org/10.1177/0002764218787854

Metselaar, S. (2019). Commentary 1: Informed consent of research participants: The gap between regulations and reality. *Journal of Empirical Research on Human Research Ethics*, *14*(5), 433–435. https://doi.org/10.1177/1556264619831589a

Mihinjac, M., & Saville, G. (2019). Third-generation crime prevention through environmental design (CPTED). *Social Sciences*, *8*(6), 1–20. https://doi.org/10.3390/socsci8060182

Minastireanu, E.-A., & Mesnita, G. (2019). An analysis of the most used machine learning algorithms for online fraud detection. *Informatica Economica*, *23*(1), 5–16. https://doi.org/10.12948/issn14531305/23.1.2019.01

Ming-Li, H., & Shun-Yung, K. W. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. *International Journal of Cyber Criminology*, *12*(1), 333–352. https://doi.org/10.5281/zenodo.1467935

Mishra, S., & Dey, A. K. (2021). Wish to craft a qualitative case study research? *South Asian Journal of Business and Management Cases*, *10*(3), 239–242. http://doi.org/10.1177/22779779211052145

Moid, S. (2018). Fighting cybercrimes using forensic accounting: A tool to enhance operational efficiency. *Wealth: International Journal of Money, Banking & Finance*, *7*(3), 92–99. http://www.ijmbf-wealth.org

Montague, D. (2010). *Essentials of online payment security and fraud prevention*. John Wiley & Sons. http://doi.org/10.1002/9781118386750

Moody's Investors Service, Inc. (2021). https://www.moodys.com/

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection, and analysis. *European Journal of General Practice*, *24*(1), 9–18. https://doi.org/10.1080/13814788.2017.1375091

Munthe-Kaas, H., Bohren, M. A., Glenton, C., Lewin, S., Noyes, J., Tunçalp, O., Booth, A., Garside, R., Colvin, C. J., Wainwright, M., Rashidian, A., Flottorp, S., & Carlsen, B. (2018). Applying grade-cerqual to qualitative evidence synthesis findings—paper 3: How to assess methodological limitations. *Implementation Science*, *13*(S1), 25–32. https://doi.org/10.1186/s13012-017-0690-9

Nadiia, S., & Snizhana, R. (2020). Internet fraud and transnational organized crime. *Juridical Tribune*, *10*(1), 162–172. http://www.tribunajuridica.eu

Nascimento, D. C., Barbosa, B., Perez, A. M., Caires, D. O., Hirama, E., Ramos, P. L., & Louzada, F. (2019, September). Risk management in e-commerce—A fraud study case using acoustic analysis through its complexity. *Entropy*, *21*(11), 1–12. https://doi.org/10.3390/e21111087

Nasr, M., Farrag, M., & Nasr, M. (2020). E-payment systems risks, opportunities, and challenges for improved results in e-business. *International Journal of Intelligent Computing and Information Sciences*, *20*(1), 1–20. https://doi.org/10.21608/ijicis.2020.31514.1018

Natow, R. S. (2019, February). The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research*, *20*(2), 160–173. https://doi.org/10.1177/1468794119830077

Newman, O. (1972). *Defensible space: Crime prevention through urban design*. Division of Macmillan Publishing Co.

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence-Based Nursing*, *22*(3), 67–68. https://doi.org/10.1136/ebnurs-2019-103145

Office for Human Research Protection. (2018). The Belmont Report. *U.S. Department of Health & Human Services*. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

Oghazi, P., Karlsson, S., Hellstrom, D., Mostaghel, R., & Sattari, S. (2021). From Mars to Venus: Alteration of trust and reputation in online shopping. *Journal of Innovation & Knowledge*, *6*(4), 197–202. https://doi.org/10.1016/j.jik.2020.06.002

O'Leary, D. E. (2019). What phishing emails reveal: An exploratory analysis of phishing attempts using text analyzes. *SSRN Electronic* Journal, *33*(3), 285–307. https://doi.org/10.2308/isys-52481

Olivero, N., Greco, A., Annoni, A., Steca, P., & Lowry, P. B. (2019). Does the opportunity make the thief? Abilities and moral disengagement in illegal downloading. *Behavior & Information Technology*, *38*(12), 1273–1289. https://doi.org/10.1080/0144929X.2019.1583768

Olowolayemo, A., Adewale, N., Zeki, A. M., & Ahmad, Z. (2019). Examining users' understanding of security failures in EMV smart card payment systems. *JOIV: International Journal on Informatics Visualization*, *3*(2), 185–191. https://doi.org/10.30630/joiv.3.2.244

Olowookere, T. A., & Adewale, O. S. (2020). A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. *Scientific African*, *8*, 1–15. https://doi.org/10.1016/j.sciaf.2020.e00464

Pabian, A., Pabian, B., & Reformat, B. (2020). E-customer security as a social value in the sphere of sustainability. *Sustainability*, *12*(24), 1–14. https://doi.org/10.3390/su122410590

Paraskevas, A., & Brookes, M. (2018, August). Nodes, guardians, and signs: Raising barriers to human trafficking in the tourism industry. *Tourism Management*, *67*, 147–156. https://doi.org/10.1016/j.tourman.2018.01.017

Peesker, K. M., Ryals, L. J., Rich, G. A., & Boehnke, S. E. (2019). A qualitative study of leader behaviors perceived to enable salesperson performance. *Journal of Personal Selling & Sales Management*, *39*(4), 319–333. https://doi.org/10.1080/08853134.2019.1596816

Peterson, J. S. (2019). Presenting a qualitative study: A reviewer's perspective. *Gifted Child Quarterly*, *63*(3), 147–158. https://doi.org/10.1177/0016986219844789

Phillippi, J., & Lauderdale, J. (2018). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research*, *28*(3), 381–388. https://doi.org/10.1177/1049732317697102

Phillips, M., & Lu, J. (2018, July). A quick look at NVivo. *Journal of Electronic Resources Librarianship*, *30*(2), 104–106. https://doi.org/10.1080/1941126x.2018.1465535

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100-million-dollar data breach. *Journal of Information Technology Teaching Cases*, *8*(1), 9–23. https://doi.org/10.1057/s41266-017-0028-0

Piroozfar, P., Farr, E. R. P., Aboagye-Nimo, E., & Osei-Berchie, J. (2019). Crime prevention in urban spaces through environmental design: A critical UK perspective. *Cities*, *95*, 1–11. https://doi.org/10.1016/j.cities.2019.102411

Poole, V. B., Corkern, S., & Hoffman, H. (2018). Prevention and resolution for identity theft: practical advice for individuals, business owners, and tax professionals. *Business Education Innovation Journal*, *10*(1), 80–86. http://www.beijournal.com/

Prenzler, T. (2019). What works in fraud prevention: A review of real-world intervention projects. *Journal of Criminological Research, Policy, and Practice*, *6*(1), 83–96. https://doi.org/10.1108/jcrpp-04-2019-0026

Priyangaa, A., Owaiseahmed, A., Kumaresan, A., & Vijayakumar, K. (2017). Detection fraudulent of credit card application using payment gateway. *Advances in Natural and Applied Sciences*, *11*(6), 103–108. http://www.aensiweb.com/ANAS

Randa, R., & Reyns, B. W. (2020). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the national crime victimization survey. *Deviant Behavior*, *41*(10), 1290–1304. https://doi.org/10.1080/01639625.2019.1612980

Reppetto, T. A. (1976, April). Crime prevention and the displacement phenomenon. *Crime & Delinquency*, *22*(2), 166–177. https://doi.org/10.1177/001112877602200204

Rettke, H., Pretto, M., Spichiger, E., Frei, I. A., & Spirig, R. (2018). Using reflexive thinking to establish rigor in qualitative research. *Nursing Research*, *67*(6), 490–

497. https://doi.org/10.1097/nnr.0000000000000307

Richardson, J. (2020). Is there a silver bullet to stop cybercrime? *Computer Fraud & Security*, *2020*(5), 6–8. https://doi.org/10.1016/S1361-3723(20)30050-6

Ross, M. W., Iguchi, M. Y., & Panicker, S. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist*, *73*(2), 138–145. https://doi.org/10.1037/amp0000240

Roulston, K. (2018). Qualitative interviewing and epistemics. *Qualitative Research*, *18*(3), 322–341. doi:10.1177/1468794117721738

Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130–157. https://doi:10.1016/j.engappai.2018.07

Sadgali, I., Sael, N., & Benabbou, F. (2020). Adaptive model for credit card fraud detection. *International Journal of Interactive Mobile Technologies* (iJIM), *14*(03), 54–65. https://doi.org/10.3991/ijim.v14i03.11763

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019, August). Deterrence and prevention-based framework to mitigate information security insider threats in organizations. *Future Generation Computer Systems*, *97*, 587–597. https://doi.org/10.1016/j.future.2019.03.024

Saia, R., & Carta, S. (2019). Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. *Future Generation Computer Systems*, *93*, 18–32. https://doi.org/10.1016/j.future.2018.10.016

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018, July). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Scott, M. S. (2018, September). Effective policing through regulatory control. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 86–104. https://doi.org/10.1177/0002716218778780

Shane, J. M., Piza, E. L., & Silva, J. R. (2018). Piracy for ransom: The implications for situational crime prevention. *Security Journal*, *31*(2), 548–569. https://doi.org/10.1057/s41284-017-0115-0

Shulzhenko, N., & Romashkin, S. (2020). Internet fraud and transnational organized crime. *Juridical Tribune*, *10*(1), 162–172. http://www.tribunajuridica.eu/

Siegner, M., Hagerman, S., & Kozak, R. (2018). Going deeper with documents: A systematic review of the application of extant texts in social research on forests. *Forest Policy and Economics*, *92*, 128–135. https://doi.org/10.1016/j.forpol.2018.05.001

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018, March). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, *21*(5), 629–634. https://doi.org/10.1080/13645579.2018.1454643

Simmons, H. (2018, March). A Framework for the analysis and management of library security issues applied to Patron-property theft. *Journal of Academic Librarianship*, *44*(2), 279–286. https://doi.org/10.1016/j.acalib.2017.12.021

Singh, A., & Jain, A. (2020). Cost-sensitive metaheuristic technique for credit card fraud detection. *Journal of Information and Optimization Sciences*, *41*(6), 1319–1331. https://doi.org/10.1080/02522667.2020.1809090

Sportiello, L. (2019). "Internet of smart cards": A pocket attacks scenario. *International Journal of Critical Infrastructure Protection*, *26*, 1–15. https://doi.org/10.1016/j.ijcip.2019.05.005

Strijker, D., Bosworth, G., & Bouter, G. (2020, June). Research methods in rural studies: Qualitative, quantitative, and mixed methods. *Journal of Rural Studies*, *78*, 262–270. https://doi.org/10.1016/j.jrurstud.2020.06.007

Summers, L., & Johnson, S. D. (2017). Does the configuration of the street network influence where outdoor serious violence takes place? Using space syntax to test crime pattern theory. *Journal of Quantitative Criminology*, *33*(2), 397–420. https://doi.org/10.1007/s10940-016-9306-9

Surmiak, A. (2018). Confidentiality in qualitative research involving vulnerable participants: Researchers' perspectives. *Qualitative Social Research*, *19*(3), 393–418. https://doi.org/10.17169/fqs-19.3.3099

Sutherland, E. (1938, February). *The professional thief*. Northwestern University Pritzker School of Law. http://doi.org/10.2307/1333907

Sutherland, E. (1939, December). *Principles of criminology* (3rd ed.). Sage Publications. https://doi.org/10.1086/632724

Taddeo, M. (2018a). Deterrence and norms to foster stability in cyberspace. *Philosophy & Technology*, *31*(3), 323–329. https://doi.org/10.1007/s13347-018-0328-0

Taddeo, M. (2018b). The limits of deterrence theory in cyberspace. *Philosophy & Technology*, *31*(3), 339. https://doi.org/10.1007/s13347-017-0290-2

Taha, A. A., & Malebary, S. J. (2020, February). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. *IEEE Access*, *8*, 25579–25587. https://doi.org/10.1109/ACCESS.2020.2971354

Tannenbaum, F. (1938, January). *Crime and the community*. Columbia University Press. http://doi.org/10.2307/2262683

Tilley, N. (2018, August). Privatizing crime control. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 55–71. https://doi.org/10.1177/0002716218775045

Tomaszewski, L. E., Zarestky, J., & Gonzalez, E. (2020). Planning qualitative research: Design and decision making for new researchers. *International Journal of Qualitative Methods*, *19*, 1–7. https://doi.org/10.1177/1609406920967174

Tripathi, D., Sharma, Y., Lone, T., & Dwivedi, S. (2018). Credit card fraud detection using local outlier factor. *International Journal of Pure and Applied Mathematics*, *118*(7), 229–234. http://www.ijpam.eu

Ucci, D., Aniello, L., & Baldoni, R. (2019, March). Survey of machine learning techniques for malware analysis. *Computers & Security*, *81*, 123–147. https://doi.org/10.1016/j.cose.2018.11.001

Usman, L. M. (2018). Terrorism and female teacher leadership in girls' secondary school. *International Journal of Educational Management*, *32*(4), 669–688. https://doi.org/10.1108/IJEM-04-2017-0084

Vakili, M. M., & Jahangiri, N. (2018, March). Content validity and reliability of the measurement tools in educational, behavioral, and health sciences research. *Journal of Medical Education Development*, *10*(28), 106–118. https://doi.org/10.29252/edcj.10.28.106

Van Puyvelde, D. (2018, November). Qualitative research interviews and the study of national security intelligence. *International Studies Perspectives*, *19*(4), 375–391. https://doi.org/10.1093/isp/eky001

Vargas, V.-M. (2019, May). The new economic good: Your own personal data. An integrative analysis of the dark web. *Proceedings of the International Conference on Business Excellence*, *13*(1), 1216–1226. https://doi.org/10.2478/picbe-2019-0107

Wadams, M., & Park, T. (2018). Qualitative research in correctional settings: Researcher bias, western ideological influences, and social justice. *Journal of Forensic Nursing*, *14*(2), 72–79. https://doi.org/10.1097/JFN.0000000000000199

Wang, P., D'Cruze, H., & Wood, D. (2019). Economic costs and impacts of business data breaches. *Issues in Information Systems*, *20*(2), 162–171. https://doi.org/10.48009/2_iis_2019_162-171

Wang, Z., Liu, L., Zhou, H., & Lan, M. (2019). Crime geographical displacement: Testing its potential contribution to crime prediction. *ISPRS International Journal of Geo-Information*, *8*(9), 1–12. https://doi.org/10.3390/ijgi8090383

Ward, J. T., McConaghy, M., & Bennett, J. Z. (2018, April). Differential applicability of criminological theories to individuals? The case of social learning vis-a-vis social control. *Crime & Delinquency*, *64*(4), 510–541. https://doi.org/10.1177/0011128717707716

Welsh, B. C., Zimmerman, G. M., & Zane, S. N. (2018, January). The centrality of theory in modern-day crime prevention: Developments, challenges, and opportunities. *Justice Quarterly*, *35*(1), 139–161. https://doi.org/10.1080/07418825.2017.1300312

Wilner, A. S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, *43*(2), 245–280. https://doi.org/10.1080/01402390.2018.1563779

Wixted, J. T., Mickes, L., & Fisher, R. P. (2018). Rethinking the reliability of eyewitness memory. *Perspectives on Psychological Science*, *13*(3), 324–335. https://doi.org/10.1177/1745691617734878

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial

populations in Malaysia. *Qualitative Report*, *23*(11), 2700–2713. https://nsuworks.nova.edu/tqr/

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

Yu, F. (2019, June). An interactive visual system for generating striking pseudo base stations decisions. *Journal of Physics: Conference Series*, *1237*(5), 1–7. https://doi.org/10.1088/1742-6596/1237/5/052019

Zanin, M., Romance, M., Moral, S., & Criado, R. (2018). Credit card fraud detection through parenclitic network analysis. *Complexity*, *2018*, 1–9. https://doi.org/10.1155/2018/5764370

Zhang, J., Gardner, R., & Vukotic, I. (2019). Anomaly detection in wide area network meshes using two machine learning algorithms. *Future Generation Computer Systems*, *93*, 418–426. https://doi.org/10.1016/j.future.2018.07.023

Zhang, X., Han, Y., Xu, W., & Wang, Q. (2019, May). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. *Information Sciences*, *518*(5), 1–15. https://doi.org/10.1016/j.ins.2019.05.023

Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges. *ACM Computing Surveys*, *54*(8), 1–36. https://doi.org/10.1145/3456628

Zuo, J. (2021). Analysis of e-commerce characteristics based on edge algorithm and cox model. *Wireless Communications & Mobile Computing*, *2021*, 1–13. https://doi.org/10.1155/2021/6628068

Appendix A: Interview Research Questions

Research Question

What successful strategies have online business leaders used to reduce revenue loss from credit card fraud?

Interview Questions

1. What are the successful strategies you used to reduce online credit card fraud?

2. What method(s) did you find work best to measure the success of your strategies?

3. What internal or external critical success factors did you consider in the design of your strategies?

4. How did you address the key obstacles in the implementation of your strategies?

5. What additional information can you share regarding your organization's experiences with strategies for reducing online credit card fraud?

Appendix B: Interview Protocol

Interview Protocol	
What to do	**What to say – The Script**
Introduce the interview. (Following the script) Remind participants of the interview's length, the use of audio recording and note-taking, and that participation is voluntary. Advise the interviewee of the participant's right to stop the interview or decline to answer any question at any time.	Hi, my name is Clarissa Rosario. How are you? Thank you for participating in this interview because your contribution is important to the online business industry. This interview will take approximately 45-60 minutes. I will record this interview to ensure that I capture your intended responses. I will also be taking notes as we go through the interview process. Please be advised that your participation today in this interview is voluntary. If there is any question that you prefer not to answer, you have the right not to. Also, be aware you can end the interview anytime you want to do so. After the interview, I will contact you again to clarify your responses and ensure that I have captured the responses you provided accurately. Are there any questions for me before we start?
Ask follow-up probing questions to gather more in-depth information. Ask the questions consistently, as written.	Initiate the interview questions: **Question 1:** What are the successful strategies you used to reduce online credit card fraud? **Question 2:** What method(s) did you find work best to measure the success of your strategies? **Question 3:** What internal or external critical success factors did you consider in the design of your strategies? **Question 4:** How did you address the key obstacles in the implementation of your strategies? **Question 5:** What additional information can you share regarding your organization's experiences with strategies for reducing online credit card fraud?
Close the Interview with the following script:	Those are all the questions I have. Thank you for taking the time to conduct this interview. Your participation is of enormous value. Next, I will transcribe and synthesize your interview responses.

Inform the participant how I will proceed and what to expect after the interview.	After your responses are transcribed and synthesized, I will email you a two-page summary of the interview, which we will use in the follow-up telephone call. I will reach out to you via email or phone call (based on your preference) to schedule another phone call session to discuss the accuracy of my interpretation of your interview responses. At that time, you can confirm your responses and expand on additional information that you feel may be valuable. This follow-up interview should take no more than 30 minutes. During this follow-up call, you will have the opportunity to review, verify, clarify, modify, or expand your responses.
Schedule member checking follow-up interview.	Let us schedule the follow-up interview call to review my accuracy in capturing your responses. When is a good day and time for us to talk for 20-30 minutes?

Appendix C: Member Checking Follow-up Interview

What to do	**What to say – The Script**
Email the transcript summary and instructions to the participant. Include additional clarification questions that emerged during the transcription of the interview.	Hi, participant name, Thank you for participating in the study. Please be advised that I have attached the interview summary to this email. Please review the summary, and we can talk about it in the scheduled follow-up interview call.
Call or email the participant (based on the participant's preference) to confirm the follow-up interview appointment.	Hi, participant name, I am calling or emailing you to confirm your availability for a follow-up interview call. Thank you again for your time and participation.
Remind the participant of the purpose of the follow-up interview and the time allocated for the follow-up interview. Review the interview summary with the participant and make updates as applicable. Ask the participant if he/she wants to expand or update any of the responses.	As I mentioned in our last interview, this is a follow-up session in which we will review my interpretations of your responses for accuracy. This discussion should not take longer than 30 minutes. Review the interview summary and make updates as applicable.
Summarize the next steps in the process.	Once the study is completed, I will let you know and send you the study's final copy. Thank you for your time and consideration. Should any questions arise, or if you would like to share any feedback, please contact me. I appreciate your time and your participation.

Appendix D: Initial Phone Call

Hi, my name is Clarissa Rosario-Tavarez. I am a Doctoral student at Walden University. I am calling to invite you to participate in a doctoral research study about strategies used by online business leaders to mitigate, prevent, and identify credit card fraud.

The criteria for selecting participants will include the following:

- Online business leaders from different companies who have successfully implemented online credit card fraud solutions.
- The leader is in the Southwest region of the United States to be in the study.

Your participation in this study is voluntary. Should you agree to participate in this study, you will be asked to answer five main questions and some follow-up clarification questions about online credit card fraud prevention strategies online business leaders use to mitigate online credit card fraud. For example:

1. What are the successful strategies and security tools you used to reduce online credit card fraud?
2. What method(s) did you find work best to measure the success of your strategy?

If you would like to participate in the research study, I would like to email you all the study information. Do I have your permission to provide me with your email to email all the information we talked about during this phone call? The email with all the information is called an invitation consent form. Please review the study consent form to decide if you would like to participate in my research study to help enhance knowledge in the business field. If you feel that you understand the research and consent to participate, please indicate your consent by replying to the email with the words "I consent."