

2020

Reducing Payment-Card Fraud

Chares R. Ross
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>



Part of the [Computer Sciences Commons](#), and the [Quantitative, Qualitative, Comparative, and Historical Methodologies Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Charles Ross

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. Diane Dusick, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Lisa Pearo, Committee Member, Doctor of Business Administration Faculty

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

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

Walden University
2020

Abstract

Reducing Payment-Card Fraud

By

Charles Ross

M.S. University of Phoenix, 2010

M.B.A, DeVry University, 2004

BS, DeVry University, 1993

Doctoral Study Submitted in Partial Fulfillment

Of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2020

Abstract

Critical public data in the United States are vulnerable to theft, creating severe financial and legal implications for payment-card acceptors. When security analysts and managers who work for payment card processing organizations implement strategies to reduce or eliminate payment-card fraud, they protect their organizations, consumers, and the local and national economy. Grounded in Cressey's fraud theory, the purpose of this qualitative single case study was to explore strategies business owners and card processors use to reduce or eliminate payment-card fraud. The participants were 3 data security analysts and 1 manager working for an international payment card processing organization with 10 years or more experience working with payment card fraud detection in the southeastern United States. The data collection process was face-to-face semistructured interviews and review of company documentation. Within-case analysis, pattern matching, and methodological triangulation were used to identify 4 themes. The key themes related to artificial intelligence, cardholder and acceptor education, enhanced security strategies, and Payment Card Industry Data Security Standard (PCI-DSS) rules and regulations to reduce or end card fraud. The key recommendations are enforcement of stricter PCI-DSS rules and regulations for accepting payment cards at the acceptor and processor levels to reduce the potential for fraud through the use of holograms and card reader clearance between customers. The implications for social change include the potential to reduce costs to consumers, reduce overhead costs for businesses, and provide price reductions for consumers. Additionally, consumers may gain a sense of security when using their payment-card for purchases.

Reducing Payment-Card Fraud

by

Charles Ross

M.S. University of Phoenix, 2010

M.B.A, DeVry University, 2004

BS, DeVry University, 1993

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

June 2020

Dedication

For Charles “Dusty” Coombs, Jr. in memoriam. You left fingerprints of grace on our lives. You will not be forgotten. Dusty, you came along at a time in my life when I was directionless and took a total stranger in. You were my advisor, my confidante, but most of all, you were a friend and mentor. Your love and support meant a lot to me; I will never forget the funny stories and some of the tall tales you told to keep me on track. All I ever had to do was make a phone call and ask if my room was available on whatever day I was coming in. You were truly more like a parent to me than my parents. After I met Dustin, you took us both under your wing. Thank you for your love and support.

Why do you cry for me

I am not there, don't cry for me

for I am with you everywhere,

I am the warm and breeze

I am the birds singing in the trees

I am the eagle that soars so high

in the blue skies, I am always and forever by your side

Don't cry for me instead rejoice for me

because in your heart I will always be

you are loved and will be missed but never forgotten

See you again one day my friend “Dusty” Coombs

Author Albert Dustin (Original Piece)

Acknowledgments

I want to thank my friends and family for their support during this journey. I would also like to thank Drs. Diane Dusick, Richard Needham, Lisa Pearo, and Geri Velkova for their input and help with the journey. A special thanks to my classmates, who made this journey enjoyable. One special thanks to a beloved friend, which we lost in 2015, without his love and support, I would not have completed this journey.

Table of Contents

Section 1: Foundation of the Study.....	1
Background of the Problem	1
Problem Statement.....	2
Purpose Statement.....	3
Nature of the Study	3
Research Question	5
Interview Questions	5
Conceptual Framework.....	6
Operational Definitions.....	6
Assumptions, Limitations, and Delimitations.....	8
Assumptions.....	8
Limitations	8
Delimitations.....	9
Significance of the Study	9
Contribution to Business Practice.....	9
Implications for Social Change.....	10
A Review of the Professional and Academic Literature.....	10
Fraud Theory and the Fraud Diamond.....	12
Fraud Triangle Theory	14
Identity Theft	20
PCI-DSS.....	26

Dark Web	33
Payment-Card Fraud Detection.....	34
Consequences of Payment Card Fraud and Data Breaches	37
Payment-Card Fraud Elimination Models (Software)	38
Chip and PIN Payment Cards	52
Transition	54
Section 2: The Project.....	56
Purpose Statement.....	56
Role of the Researcher	57
Participants.....	60
Research Method and Design	62
Research Method	63
Research Design.....	64
Population and Sampling	66
Ethical Research.....	68
Data Collection Instruments	70
Data Collection Technique	72
Data Organization Technique	74
Data Analysis	75
Reliability and Validity.....	77
Reliability.....	78
Validity	78

Transition and Summary.....	80
Section 3: Application to Professional Practice and Implications for Change	82
Introduction.....	82
Presentation of the Findings.....	82
Emergent Theme 1: Artificial Intelligence	83
Emergent Theme 2: Cardholder and Acceptor Education	86
Emergent Theme 3: Enhanced Wireless Security Strategies	91
Emergent Theme 4: PCI-DSS Rules and Regulations.....	94
Applications to Professional Practice	97
Implications for Social Change.....	99
Recommendations for Action	100
Recommendations for Further Research.....	101
Reflections	102
Conclusion	103
References.....	105
Appendix A: Explanation of Card Stripes Track 1	133
Appendix B: Explanation of Card Stripes Track 2	134
Appendix C: Cover Letter.....	135
Appendix D: Consent Form.....	136
Appendix E: Interview Protocol	140
Appendix F: Interview Questions	141

List of Figures

<i>Figure 1.</i> Kassem and Higson's (2012) new fraud triangle model.....	15
<i>Figure 2.</i> Dilla et al. depiction of fraud diamond (2013).....	18
<i>Figure 3.</i> Conceptual model of identity definitions (Jamieson et al., 2012).	25

Section 1: Foundation of the Study

Media reports on payment-card data breaches lead consumers to believe retail companies should provide secure transactions without the fear of thieves obtaining the cardholders' data (Chang, Venkatasubramanian, West, & Lee, 2013). However, retailers and bankers face the problem of theft of customer information during transmissions of payment-card data every day (Chang et al., 2013). More than 15 million people have their identity stolen through card readers and automated teller machines annually (Chang et al., 2013). According to the Trustwave Global Security Report (Trustwave, 2016), retail businesses accounted for 60% of the payment-card data breaches. Thieves obtain information from the stripe on the back of the customer's card using skimming techniques (Fossi et al., 2009). Since the advent of e-commerce web sites, data breaches and identity theft have increased (Hoffman, 2013). The purpose of this qualitative single case study was to explore strategies business owners use to minimize payment-card fraud.

Background of the Problem

Identity theft involves taking on another person's identity for financial gain (Tan, Guo, Cahalane, & Cheng, 2016). Tan et al. (2016) stated that retailers lose an estimated \$3.5 billion in lost revenue due to financial card transaction fraud. Payment acceptors' network security infrastructures are not up to date, which allows criminals to capture card information. While the dollar amounts retailers lose is significant, the victims and the card issuers experience a variety of adverse effects (Cross & Kelly, 2016).

The effect on the victims includes physical health and well-being, financial trauma, depression, and psychological traumas (Cross & Kelly, 2016). However, globally, card issuers look for new methods to detect fraud and reduce organizational costs, both fiscally and reputationally (Cross & Kelly, 2016). Canadian, European, and United States card issuers have implemented the chip and pin technology, but card issuers in the European Union and the United States still experience fraudulent data breaches (Canadian Bankers Association, 2014).

Payment-card fraud is one of the most significant threats to business on a national and international basis (Gold, 2014). Customers of major retailers, banks, and hospitality services face the possibility of fraudulent card activity (Berezina, Cobanoglu, Miller, & Kwansa, 2010) when presenting their card to pay for services or merchandise at brick and mortar or online retailers. However, incidents of a data breach and payment-card fraud have occurred at the merchant level at businesses such as Target, Sally's Beauty Supply (a nationwide beauty supply company), Home Depot, and Neiman Marcus that are changing the customers' feelings of security (Hardekopf, 2015).

Problem Statement

Critical public data in the United States are vulnerable to theft, creating severe financial and legal implications for payment-card acceptors (Sen & Borle, 2015). The cost of identity theft to online and brick and mortar retailers was approximately \$16.31 billion in 2014 (Vona, 2015). The general business problem was that payment-card acceptors and processors do not incorporate strategic systems to prevent card fraud and

identity theft at the card processing organization. The specific business problem was that some international card processing organization managers lack strategies to minimize payment-card fraud.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies international card processing organizations use to minimize payment-card fraud. The targeted population was five to eight data security specialists working for an international card processing organization in the southeast United States who have successfully prevented data breaches and payment-card fraud. The implication for positive social change included the potential for lowering the number of data breaches and payment-card fraud instances, which could provide customers with confidence in using their payment cards, reduce fraud losses, and thereby improve the economy.

Nature of the Study

Researchers may choose from three methods: quantitative, qualitative, and mixed method. Qualitative researchers collect data by exploring documents, observing, and interviewing interview participants (Marshall, Cardon, Poddar, & Fontenot, 2013). A quantitative researcher may target the amount of data, allowing for a broad cross-section and a large volume of numerical data to analyze (Vaitkevicius & Kazokiene, 2013). Quantitative researchers use close-ended questions to test hypotheses and do not allow for added probing (Vaitkevicius & Kazokiene, 2013). Mixed-method research may enhance the gain made by both methods; however, mixed-method research needs

considerable investigative skills and creates additional time and information refining (Venkatesh, Brown, & Bala, 2013). The use of a qualitative research method enabled the collection of rich and thick data to discover the successful strategies that security specialists in international card processing organizations in the Southeast United States use to prevent data breaches and payment-card fraud.

Under consideration were three qualitative design strategies (a) single case, (b) phenomenology, and (c) ethnography. The single qualitative case study approach offers abundant opportunities to the researcher for learning and provided the ability to inform or generate theory (Hart, 2013). A single case study design was chosen to focus on the issue of payment card fraud reduction. Case study researchers focus on exploring a specific phenomenon thoroughly, using a representative or typical case (Yin, 2014).

Phenomenological research entails collecting data about the human experience, with an emphasis on subjectivity (Moustakas, 1994). By contrast, the narrative itself is the object of interest to narrative researchers (Yin, 2014).

As the purpose of this study was to explore strategies business owners can institute to minimize payment-card fraud, the single case study design was most appropriate. A phenomenological design was not suitable for this study because the goal was not to explore participant's lived experiences (Moustakas, 1994). An ethnographic study was not suitable for this study because the purpose of the study did not require field observations; also, the time required to conduct an ethnographic study would have been prohibitive.

Research Question

The goal of the study was to address one primary research question:

RQ1: What strategies do international card processing organization managers use to minimize payment-card fraud?

Interview Questions

The following conceptualized interview questions aided in data collection:

1. What opportunities still exist for a person to commit payment-card fraud at the card processing level?
2. What legal strategies do you see organizations taking to protect themselves from monetary loss from data breaches?
3. What plans do you have to implement payment-card security?
4. How has your organization increased security to reduce those opportunities?
5. There are separate ways for card acceptors to combat fraud. What technology tools has your organization implemented?
6. What strategies have you implemented or planning to make your payment-card protection strategy stronger and yet less costly for your company?
7. How useful are the tools and strategies your organization has implemented?
8. What changes in the PCI-DSS standards need to be added that could increase security?
9. What steps can payment-card acceptors take to increase security for accepting payment cards?

10. If you implemented fraud-detection practices, what problems did you meet during the conversion?
11. What else can you add about strategies that the payment-card acceptors could implement to reduce and eliminate fraud and identity theft?

Conceptual Framework

The theory that served as the conceptual framework for this study was the fraud theory, which was proposed by Cressey in the 1950s (Cressey, 1954). Cressey (1954) developed the fraud theory to describe (a) why people commit fraud, (b) the rationalization people use for having committed fraud, and (c) the financial need of individuals who commit fraud. Fleming, Hermanson, Kranacher, and Riley (2016) further defined Cressey's fraud theory stating that people commit fraud because of (a) opportunities, (b) rationalizations, and (c) peer pressure. The critical concepts of fraud theory include fraud risk assessment, rationalizing the act, and the person's motivation to commit fraud. As applied to this study, fraud theory was right for the study because it allowed the participants to effectively explore perceptions and experiences regarding strategies to reduce payment-card fraud opportunities.

Operational Definitions

Botnet: Botnets are a network formed of hosts controlled remotely by a bot-master to spread malicious viruses to a network (Narang, Hota, & Sencar, 2016).

Card not present: Card not present transactions are transactions performed when the cardholder is not present such as Internet, mail-order, or telephone purchases (Sahin, Bulkan, & Duman, 2013).

Card present: Card present is the offense of using a payment-card to buy something with the knowledge that the forged or stolen payment-card has been revoked or canceled or the card's use is unauthorized (Card Present, 2014).

Denial of service: Denial of service refers to botnet attacks on Internet servers through remote command to perform malicious attacks by the bot-master and denies service to other servers (Wang, Lin, Cheng, & Chen, 2017).

Identity theft: Identity theft is the act of stealing a person's identity for unlawful gains (McNally, 2008).

Malware POS–point of sale: POS malware is a powerful software used to illegally obtain payment-card datum (Steer, 2014).

Phishing: Phishing refers to attaching fake information websites using e-mails to obtain a person's personal data (Kim, Sefcik, & Bradway, 2016).

Vishing: Vishing refers to phone deception requiring phone answerers to enter their payment-card or checking account information by the phone keypad to clear up some financial problem (Mugari, Gona, Maunga, & Chiyambiro, 2016).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are the elements the researcher assumes to be true without evidence (Ellis & Levy, 2009). Three assumptions were the basis of the study. The first assumption was that the participants would supply honest and detailed descriptions in response to the interview questions. The second assumption was the qualitative single case study was the best design to address the research question and to collect that data, that the senior managers would provide access to the supporting documents and data. The last assumption was that the participants were knowledgeable and willing to impart information about how the company currently handles payment-card fraud.

Limitations

Limitations are internal threats to any study's validity (Ellis & Levy, 2009). The first limitation of the study was the willingness of the senior managers to take part in the study. Because the study was conducted at a single company in the southeastern United States, the strategies for card fraud detection may not be representative of other payment card processing organizations located in the United States. The results of the study are limited by the willingness of the participants to share their knowledge and organization documents, the thoroughness of their responses, and the ability to recruit a sufficient number of participants to achieve data saturation.

Delimitations

Delimitations are the stated boundaries of the study (Ellis & Levy, 2009). The delimitations set the scholarly tone of the research and define what the research leaves out (Ellis & Levy, 2009). The participants were data-security specialists at an international payment-card processing organization in Georgia. Only data-security specialists with a minimum of a bachelor's degree and a minimum of 10 years of experience in their respective fields took part in the study.

Significance of the Study

The results of the study may provide data-security experts with answers on how to prevent payment-card fraud. The results of the study may create incentives for business owners to follow payment-card industry data-security standard (PCI-DSS) recommendations. The PCI-DSS incentives include (a) reduced liability, (b) reduced revenue loss, (c) potential reduction in costs to consumers for products or services, (d) increased consumer confidence leading to increased tax bases, (e) increased tax bases that may lead to infrastructure improvements and (f) an increased workforce. The findings of this study may also add value to businesses by enhancing card acceptors' and processors' ability to increase card security and reduce fraud opportunities.

Contribution to Business Practice

The results of this study have a practical business application. The results of the study may increase business leaders' awareness of the strategies needed to reduce payment-card fraud opportunities. The results of this study could serve as a guide for

senior card processing organizations' managers and card acceptors to reduce card fraud by obtaining the knowledge of how to reduce fraud opportunities. Card acceptors may increase POS security through enhanced technological advances that may result in a reduction in payment-card fraud.

Implications for Social Change

The results of this study may have implications for social change. One implication for positive social change is that the findings of this study may provide practical strategies for card processing organizations' senior managers to reduce card fraud opportunities. The results might supply strategies to motivate card acceptors to increase payment-card security; thereby, increasing consumer confidence in the card acceptors' ability to provide secure transactions. Increasing confidence in payment-card security in retail businesses may enable the leaders of retail organizations to prepare for and deter the malware and viral attacks on the POS systems; thereby, deterring payment-card fraud and identity theft. The results of the study may influence the belief of payment-card acceptors globally, both directly and indirectly.

A Review of the Professional and Academic Literature

Payment-card fraud and data breaches occur daily in diverse types of businesses. Card transaction processors meet fraudulent transactions daily due to card acceptors not having the appropriate strategies to detect fraud. Suman (2014) presented an overview of distinct types of business fraud to include (a) payment-card, (b) telecommunication, (c) data breach, (d) bankruptcy fraud, (e) theft counterfeit, and (f) application fraud. Suman

defined payment-card fraud as online and offline unauthorized usage of another person's card.

A data breach is the act of entering without warrant or invitation to another computer system or network. Theft counterfeit fraud is the same type of fraud where the person uses another's card without permission (Suman, 2014). Application fraud is the act of applying for credit or employment in another person's name and using that person's credentials (Suman, 2014). The three types of fraud defined by Suman (2014) examined in this study are (a) payment-card fraud, (b) identity theft, and (c) data breaches resulting in payment-card information theft.

The comprehensive literature review includes an exploration of relevant topics to supply a scholarly background that supports the need to address the problem of payment-card fraud elimination. The literature review includes the topics of (a) fraud theory, (b) fraud triangle theory, (c) identity theft, (d) payment-card fraud detection, and (e) payment-card fraud elimination models. Search keywords used included (a) *credit card fraud*, (b) *identity theft*, (c) *credit card fraud elimination*, (d) *credit card fraud detection*, (e) *fraud theory*, and (f) *fraud triangle theories*. Other keyword searches included *computer crimes*, *swindling*, *Internet fraud*, and *economic crime*.

The sources were articles in peer-reviewed journals from Walden University Library and Google Scholar using EBSCOhost, ProQuest, Science Direct, and Thoreau. The resulting review provided useful data to respond to the research question with primary sources published from 2014 to 2018 to ensure this study had a supported

research method and design. Of the more than 150 sources; 90% are within the last 5 years.

The focus of this qualitative case study was to examine the strategies card processing companies use to determine fraudulent card transactions. Fraud theory and the fraud diamond were the foundation for determining card fraud. Omar, Nawawi, and Puteh Salin (2016) discussed fraud theory as the theory that pertains to American card fraud. The review includes global and American sources for card fraud detection. The primary focus; however, was on American card-fraud and data breaches.

Fraud Theory and the Fraud Diamond

Cressey developed fraud theory in 1950 and revised the theory in 1954. Fraud theory offers researchers and business leaders three potential reasons for a person to commit fraud (a) opportunity, (b) rationalization and, (c) financial gain (Cressey, 1950). Tan et al. (2016) defined fraud as involving the use of fabricated identity for financial gain. Fraud theory is the foundation for the fraud triangle theory. Fraud theory, which is relevant to payment-card fraud, enables corporate auditors to determine fraudulent financial transactions in corporate America (Omar et al., 2016).

Fleming et al. (2016) proposed three reasons people commit fraud (a) financial problems, (b) opportunity, or (c) rationalization (i.e., company owes them something in the individual's mind). Omar et al. (2016) noted that financial distress, as perceived by the individual, is one of the leading causes of fraud. The perpetrator may be unwilling to discuss financial problems and may have a powerful sense of ego, preventing that person

from discussing why he or she felt compelled to commit the fraudulent act (Fleming et al., 2016). Personal financial problems lead people to commit fraud without considering the consequences.

Fleming et al. (2016) discussed how fraudsters justify committing fraud through (a) a moral justification, (b) feeling the organization owes them something, and (c) rationalization. Fleming et al. reported that fraudsters justify committing fraudulent acts as part of their moral comfort zone. Fraudsters rationalize the theft by claiming the business owes them for poor working conditions (Omar et al., 2016). The fraudster rationalizes his actions because he feels the company owes him either for his demanding work or through managerial changes.

Omar et al. (2016) stated that the person committing the fraudulent act has a slim chance of capture. The person committing fraud may use the payment-card for several small purchases or one large luxury purchase (Fleming et al., 2016). The completion of fraudulent purchases occurs before the victim tries to use their account to make a purchase. Payment-card fraudsters realize the act of committing fraud needs both ability and the belief that he or she may not be caught (Craig & Piquero, 2016; Omar et al., 2016).

In summary, the purpose of this study was to explore strategies that business owners and card processors use to reduce or end payment-card fraud. Fraud theory provides a foundation for understanding why and how thieves commit fraud. Finding opportunities for a person to commit fraud is the first step in reducing or eliminating

payment-card fraud. Cressey (1950, 1954) expanded on fraud theory by creating the fraud triangle theory, which is covered in the next section.

Fraud Triangle Theory

Cressey (1950, 1954) and Fleming et al. (2016) explained the fraud triangle as (a) opportunity, (b) rationalization, and (c) financial pressure. Business owners, managers, and card acceptors focus on the opportunities for a person to commit card fraud. Omar et al. (2016) analyzed the *fraud triangle* as a model for assessing the risk of fraud opportunities, but the triangle is only one aspect of the risk assessment plan. Identifying fraud risk is a significant part of assurance services. Fleming et al. stated the triangle of fraud action includes (a) the act, (b) concealment, and (c) conversion. The act of committing fraud is the execution and method of fraud. The concealment constitutes hiding the action, and conversion represents the process of turning the ill-gotten gains into something tangible by the criminal.

Cressey (1950, 1954) created the fraud triangle theory after interviewing 250 prisoners in 1950. Cressey (1950) defined the fraud triangle by the reason's fraudsters commit fraudulent acts. Abdullahi and Mansor (2015) discussed Cressey's fraud diamond. The fraud diamond, according to Abdullahi and Mansor included pressure, opportunity, and rationalization. The perceived pressures, incentives, and motives refer to factors that lead to unethical behaviors. Abdullahi and Mansor stated every fraud perpetrator faces some form of pressure to commit fraud. The opportunity presents itself through the lack of controls (internal and external in an organization), and unethical

employees may seize the opportunity to commit the felonious act (Abdullahi & Mansor, 2015). The rationale for a person to commit fraud refers to the justification and excuses to commit the unethical behavior (Abdullahi & Mansor, 2015). Figure 1 portrays Cressey's Fraud Triangle with Kassem and Higson's updated version of 2012.

Abdullahi and Mansor (2015) discussed the pressure a potential fraudster feels to commit the act. The pressures (i.e., motives) to commit fraud become the heat source for the act (Abdullahi & Mansor, 2015). Pressures may include ways to pay for a more opulent lifestyle, employment pressures, or the organization's fiscal interests (Abdullahi & Mansor, 2015). More pressures may be external (a) business financial stability, (b) high management turnover rate, or (c) lack of segregation of duties (Abdullahi & Mansor, 2015).

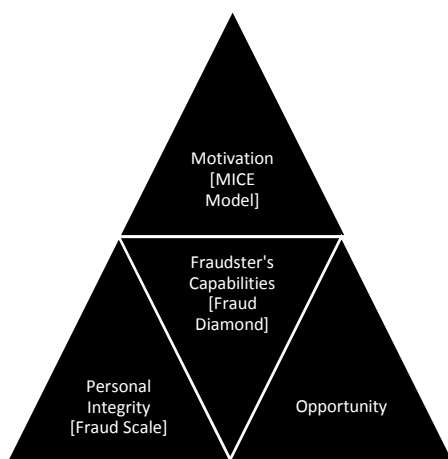


Figure 1. Kassem and Higson's (2012) new fraud triangle model.

Note: Kassem and Higson's new fraud triangle model is an expansion to Cressey's Fraud Triangle notating (a) motivation, (b) capability, (c) opportunity, and (d) personal integrity. Adapted from: "The new fraud triangle model" by R. Kassem and R.

W. Higson, 2012, *Journal of Emerging Trends in Economics and Management Science*, 3(3), p. 194. Reprinted with permission from Kassem.

Although Abdullahi and Mansor (2015) portrayed the new fraud triangle in their study, Lokanan (2015) challenged the fraud triangle and the usefulness of the triangle. Lokanan stated the fraud triangle should not be a single reliable model for anti-fraud professionals. Lokanan argued that the fraud triangle is a theoretical anchor, and the fraud triangle endorses a body of knowledge that lacks objective criteria. The body of knowledge basis comes from the individual's moral makeup and ethical background. Lokanan referred to Fleming et al.'s 2016 study as a foundational framework of the new fraud triangle.

Boyle, DeZoort, and Hermanson (2015) evaluated the use of alternative fraud model practices affecting professional audit standards. Boyle et al.'s analysis focused on the auditor's approach to fraud, including how the auditor used the fraud triangle and the effectiveness of the clients' anti-fraud measures. Boyle et al. listed anti-fraud measures (a) deterrence, (b) prevention, (c) detection, and (d) procedures. Fraud deterrence measures involve the controls and probability of fraudulent activity. Fraud prevention measures include audits, data security, and monitoring activity (Boyle et al., 2015). Fraud detection organizations follow PCI-DSS rules and regulations (Boyle et al., 2015; Willey & White, 2013). Fraud deterrence procedures involve eliminating that may cause fraud in comparison to prevention identifying and stopping existing fraud activity (Boyle et al., 2015).

The measures described by Boyle et al. (2015) follow Cressey's 1950 fraud triangle model and make a distinction. The distinction discussed by Boyle et al. indicated a company may have healthy internal fraud controls and yet the criminal may not have a strong perception of the controls. Cressey's fraud triangle, or fraud diamond, consider business, personal, and peer pressure reasons for one to commit fraudulent acts.

Azrina and Ling Lai (2014) defined the fraud diamond as opportunity, motivation, capability, and rationalization. Dilla, Harrison, Mennecke, and Janvrin (2013) described how the fraud diamond aspect of the fraud triangle applies to the virtual world. The virtual four-sided diamond includes (a) opportunity, (b) motivation, (c) business record-keeping and (d) virtual laboratories for risk assessment. The four sides of the diamond represent the criminals' capacities in the virtual world (Dilla et al., 2013). Mui and Mailley (2015) discussed the comparison of the fraud triangle and the fraud diamond. The fraud diamond shares the same characteristics with one difference – why the person commits fraud.

The fraud diamond described by Mui and Mailley (2015) includes (a) opportunity, (b) motivation, (c) rationalization, and (d) reason for the person to commit. The societal factors include philosophical and religious tradition, culture, social norms, and the rule of law, socio-economic conditions, and political status - relate to the environment where the perpetrator resides and have an effect on the disposition of the perpetrator (Mui & Mailley, 2015). The difference between the fraud diamond and the fraud triangle described by Mui and Mailley is societal factors. Auditors and fraud prevention

personnel use both the triangle and the diamond to understand why a person commits fraud.

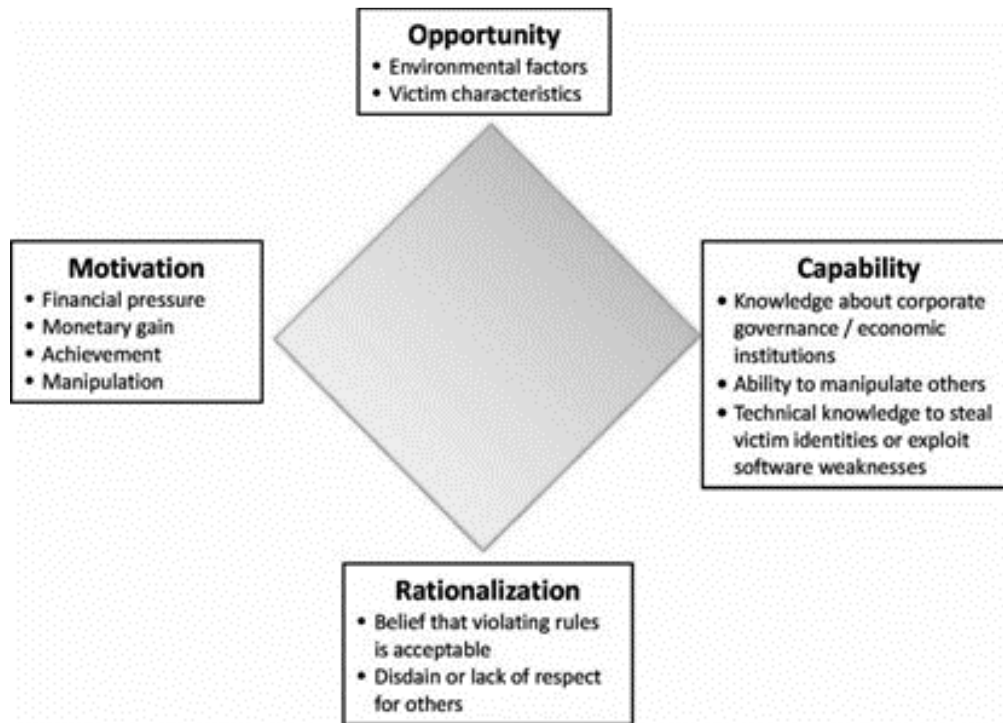


Figure 2. Dilla et al. depiction of fraud diamond (2013).

Note: Adapted from “The assets are virtual, but the behavior is real: An analysis of fraud in virtual worlds and its implications for the real world”. By Dilla et al. 2013, *Journal of Information Systems*, 27, 131-158. Reprint with permission from the authors.

In summary, payment-card fraud occurs through opportunity according to the information provided in fraud and fraud triangle theories (Schuchter & Levi, 2015). The person committing the fraudulent transaction feels perceived pressure due to the opportunity and motivation (Schuchter & Levi, 2015). Schuchter and Levi (2015) explained opportunity allows the thief to decide to commit fraud because of the absence

of transparency as well as the lack of discipline. The lack of transparency from the thief's perspective comes from the absence of compliance or managerial accounting (Schuchter & Levi, 2015). Lack of discipline and irresponsible corporate governance within the organization leads to a lack of audit controls, thus encouraging the crime (Schuchter & Levi, 2015). Fraud and fraud triangle theories supply insight into the fraudster's reasoning for committing fraud and identity theft. These insights supply a foundation for understanding how to prevent fraud and identity theft.

Cressey's 1973 fraud triangle theory examined the motivation for someone to commit fraud; the triangle includes (a) pressure, (b) opportunity, and (c) rationalization (Dorminey, Scott Fleming, Kranacher, & Riley, 2012). However, Dorminey et al. (2012) believed that the Fraud Triangle was only one crucial part of finding the risk of opportunities. Dorminey et al. stated that fraudsters' motivation might be expanded and identified with acronym MICE: money, ideology, coercion, and entitlement, or ego. In addition, McMahon, Pence, Bressler, and Bressler (2016), Wolf et al. (2015), and Beasley, Carcello, Hermanson, and Lapides (2000) identified a fourth critical element which they thought should be added to Cressey's Fraud Triangle. McMahon et al., Wolf et al., and Beasley et al. believed that capability was equally as important as the first three factors. Adding capability to the fraud triangle could aid in fraud prevention and detection.

Identity Theft

In this section of the review, consideration was made to studies on identity theft and payment-card fraud to define how identity theft affects payment-card fraud. Card processing organizations use the information located on a person's card to determine issuer and obtain approvals for purchases. Marcum, Higgins, Ricketts, and Wolfe (2015) determined how students in a rural North Carolina high school stole people's identity through (a) assuming someone else's appearance and (b) obtaining the victim's personal information. Impersonation of a person is not as simple as stealing a person's social security number or other personal information. Consumers should watch card usage via the issuer's website (if available) and track credit reports to ensure report accuracy.

Modi, Wiles, and Mishra (2015) and Bai and Chen (2013) reported the magnetic stripe payment cards allow criminals to commit banking fraud and identity theft. Magnetic stripe payment cards are easy to clone (Modi et al., 2015). Modi et al. explained the data recorded on the magnetic stripe are (a) cardholder name; (b) address; (c) card number; (d) CVV on the back of the card; and (e) line of credit. Magnetic stripes on payment cards have two to three tracks. Most payment cards use tracks one and two. Track one's format contains cardholder information and name and personal information (Appendix A). The data on track one for financial products have proprietary issuer data. Track 2 does not include the cardholders' names. However, track two does have similar information written in ANSI code to track one (Appendix B).

The cloning of a person's payment-card affords the criminal opportunities to commit banking fraud (Modi et al., 2015). Modi et al. (2015) described third-party and offshore payment-card processors' lack of enough security and inability for authorities to apprehend card thieves. Third-party transactions have the potential for failure because of the lack of data-security (Modi et al., 2015). The lack of safety increases failure costs at the third-party processor. Failure costs lead to increased shareholder losses (Modi et al., 2015) for the organization where a data breach has occurred.

Modi et al. (2015) performed the study using a sample of 146 customer information security breaches. Modi et al. concluded that the increase in cost to shareholders leads to decreased returns. The quantitative study by Modi et al. included samples of sensitive personal data and propensity scores for evaluating changing concerns. Propensity scores are quantitative risk measurements used to determine potential fraud (Turner, 2014). Changing concerns describe the mistakes within the fraud activity formula (Modi et al., 2015). Modi et al. described the propensity score and the changed curve as flags created within the card processing system flagging potential fraud transactions.

Bai and Chen (2013) posited that immoral persons contact bank customers using e-mail to obtain personal information. The e-mail appears as an official notice from the bank, within the body of the e-mail, the fraudster requests certain information such as the customer's card number and cell phone number. Once the cardholder supplies the information, the fraudster closes out the client's cell phone, obtains a new card, and

immediately overdraws the card (Bai & Chen, 2013). Additionally, the fraudster may use *TeamViewer* to remote into a person's computer and obtain information using key loggers. Keylogger software captures a PC user's keystrokes and provides the logger with the unsuspecting person's personal information such as passwords and logins.

Kahn and Linares-Zegarra (2016) researched how consumer behavior pertains to identity theft and fraud. Components of the Kahn and Linares-Zegarra study included physical prevention, account monitoring, agency control, password security, and risky consumer behaviors. Kahn and Linares-Zegarra found that users do not think about the actions or reactions of identity theft because of the *lack of consumer education* in the defense against identity theft and fraud. Kahn and Linares-Zegarra referred to the defense against identity theft through consumer education. Consumer education includes payment-card protection, account monitoring, password security, and avoiding risky card behavior (i.e., leaving cards and personal information unattended) (Clough, 2015; Kahn & Linares-Zegarra, 2016). Societal education about payment-card and identity theft lead the researcher into physical prevention.

Clough (2015) found that consumer naiveté is the leading cause of identity theft. Clough defined three segments of identity theft: financial, criminal, and identity cloning. Financial theft occurs when a thief portrays the victim to obtain credit from a financial institution. Criminal theft happens when the criminal identifies him or herself as another person to commit a crime, obtain special permits, or commit acts of terrorism. Identity cloning occurs when the thief uses another person's identity to assume his or her identity

in daily life to obtain new phone or wireless accounts, utility services, or other credit-related services. Clough stated that identity theft occurs both offline and online. Victims of identity and card fraud come from all backgrounds, races, and sexual orientations. Police officers and courts alike need to understand the definition of fraud and identity theft.

The courts address identity theft as an injury-in-fact as described in Article III, standing principals of the United States Constitution (Martecchini, 2016). Article III of the United States Constitution requires plaintiffs to “show concrete and particularized injury that is fairly traceable to the challenged conduct and likely to be redressed by a favorable judicial decision” (Martecchini, 2016, p. 1475). The victim of identity theft must show the justice system's proof of injury. The 7th Circuit Court of Appeals found customers whose breached payment-card data were at risk of identity theft and increased risk for fraudulent charges. Reynes and Randa (2017) described the victims of identity theft and payment card fraud as female, elderly, economic background, and race. The victim must decide to report the crime to the police.

Legal action on the municipal level is not enough to fight identity theft. Konradt, Schilling, and Werners (2016) stated that phishing is growing exponentially and has become a societal issue. Konradt et al. explained that online identity theft is hard to prove due to a lack of physical evidence. Physical evidence may include transcripts of computer chats, online purchase transaction records, or applying for credit in another

person's name (Konradt et al., 2016). With the development of WIFI, people have come to expect absolute security at locations with publicly available WIFI connections.

Virtual identity locks prevent a person(s) from stealing online identities (Konradt et al., 2016). Konradt et al. (2016) defined virtual identities as assuming someone's (a) name, (b) image, (c) e-mail, or (d) or other personal data to use by the person committing fraud. Additionally, Konradt et al. stated the person or persons who use another person's information deceives employers, credit grantors, and non-business-related persons. Knight and Saxby (2014) discussed how identity deception is a broader cause than identity theft as one of the many classes of identity crime. Identity deception allows someone to assume another person or business' identity (Knight & Saxby, 2014).

Police and judges define identity theft as the theft or assumption of a pre-existing identity with or without consent and in the case of an individual living or deceased. The United States government defines identity theft through the Identity Theft and Assumption Deterrence Act (Federal Trade Commission, 1998). The Act's introduction mitigates the economic cost to victims, both entity and individual. The consequences of identity theft include fines and or jail as a deterrent to future perpetrators (Knight & Saxby, 2014). The drafters of the Identity Theft and Assumption Deterrence Act identify identity theft as a federal crime with 15 years' imprisonment and \$250,000 in fines.



Figure 3. Conceptual model of identity definitions (Jamieson et al., 2012).

Note: Adapted from: “Addressing identity crime in crime management information systems: Definitions, classification, and empirics”. *Computer Law and Security Review*, 28, 381-395. Reprinted with permission by authors.

Knight and Saxby (2014) stated that government officials need a dependable identity-crime management program. Knight and Saxby posited the evolution of identity crimes provides ideas for new research into technological advances and new government regulations. Each state government has (a) a different definition, and (b) different judicial conviction outcomes (Knight & Saxby, 2014). Knight and Saxby posited state legislators should work together to have standard identity theft definition and common judicial outcomes. The variances in identity theft convictions are state law dependent.

In summary, identity theft and payment-card fraud provide opportunities for fraudsters to defraud victims and organizations. When a thief captures a victim’s payment-card information, the thief is capturing the information in the magnetic stripe’s track 01. The captured data provide personal information such as the victim’s name, address, social security number, and phone number(s). The fraudster, in turn, uses the

obtained information to open new accounts in the victim's name but does not use the person's phone number. The victim discovers they have been a victim of identity theft when they go to open a new line of credit or make a large purchase and learn of unpaid accounts.

PCI-DSS

In this section, a review of the security requirements established by PCI-DSS for card processors and acceptors is provided. PCI-DSS Data-Security standards set the minimum-security standards for payment-card acceptors and processors (Fernandes, 2015; Willey & White, 2013). The standards are recommended worldwide to reduce fiscal business loss from card fraud. Card providers and acceptors worldwide have accepted PCI-DSS compliance (Fernandes, 2015) as a guideline to reducing data breaches and card fraud. The requirements provide the foundation for protecting customer information from misuse. PCI-DSS, as of 2015, has 12 security requirements for protecting cardholder information (Fernandes, 2015; Willey & White, 2013). All businesses that accept or issue cards and process or transmit card data has to adhere to the PCI-DSS requirements (Fernandes, 2015).

P. Harvey (2013) and Fernandes (2015) described the requirements created by PCI-DSS as network personnel, quickly identifying who, what, when, and whether specific files were accessed. Fernandes stated in the write-up of his study that PCI-DSS compliance is necessary for all businesses that accept payment cards. PCI-DSS

compliance offers the cardholder a sense of security for businesses maintaining card data (Fernandes, 2015; Harvey, 2013).

PCI-DSS Regulations provide a written outline for organizations to increase network security, enhance business reputation and brand value, and decrease the chance of data breach (Fernandes, 2015). Compliance with PCI-DSS requirements means monitoring log files and critical files in real-time with automation (Fernandes, 2015). Automation offers the business enhanced payment-card security. However, Rees (2014) provided business leaders with another methodology for data breach cleanup and recovery. Rees discussed the controversial PCI-DSS requirements for taking card payments.

P. Harvey (2013) and Fernandes (2015) explained the 2014-15 PCI-DSS requirements for payment-card acceptors to secure cardholders' data. The recommendations are the most challenging too secure and protect customers' card information. The requirements track and monitor network resources and cardholder information and deploy detection mechanisms to alert network security professionals to intrusions (Fernandes, 2015). Rees (2014) reviewed the design of PCI-DSS to protect cardholders' information. No business wants to be the subject of a data breach where multiple people's information has been stolen.

Rees (2014) described that the cleanup costs and fines are devastating and long-term costs in damage to the organization's reputation. When properly maintained, the PCI-DSS requirements reduce the chances of a damaging data breach. Rees discussed

that if the worst happens to an organization, the company would still have the security policies and procedures to address the security event and mitigate the issue through effective countermeasures.

Business leaders often state the PCI-DSS requirements are hard and expensive to meet (Rees, 2014). The requirements can be complicated or straightforward as the security analysts for the organization want to interpret them. The cost is expensive for the purchase of infrastructure equipment (Rees, 2014). However, the equipment cost may not be as expensive as the fines and loss of business revenue. Business leaders argue that PCI-DSS requirements are not legal (Rees, 2014). The requirements indicated by Rees (2014) protect businesses of any size from data breaches or card fraud.

Rees (2014) stated that the requirements do not have to be difficult, and the implementation of security equipment expensive. The components are challenging; Rees suggested using PCI-DSS approved vendors for network and equipment scanning. The recommendation made by Rees is to choose QSA approved PCI-DSS consultants with broad experience. Although Rees made recommendations for qualified consultants, Murdoch and Anderson (2014) discussed the risk of Europay, Mastercard, and Visa's (EMV) chip and pin cards in Europe, which included the magnetic stripe and the chip on a cheap card.

Fraudsters could still easily clone the cards and capture the user's PIN. As the technology improved, the chip and pin cards introduced more serious fraud problems

through tampering with the pin (Murdoch & Anderson, 2014). Although the terminals for the cards were certified tamper-proof, the machines were not.

Severe flaws in the machine (e.g., non-tamper proof) slowed the certification process (Murdoch & Anderson, 2014). Additional areas for an attack on the chip and pin card in the early days was the relay attack during transaction processing (Murdoch & Anderson, 2014). The relay attack exploits the card authentication process of the merchant's terminal (Murdoch & Anderson, 2014). However, the card presenter did not know which terminal was processing the purchase.

Academia and corporate America look at corporate greed and fraud in different lights. Payment-card fraud determination follows PCI-DSS rules and regulations (Maroun & Atkins, 2014). Rule interpretation by data-security professionals and business leaders follow multiple paths. The implementation of the rules may be as straightforward or as complicated as management determines the need (Maroun & Atkins, 2014). The PCI-DSS rules are a guide to data-security for card acceptors (Maroun & Atkins, 2014).

Ganesan (2016) explained the PCI-DSS requirement for password protection for enterprise-wide protection. Network users tend to record their passwords in unsecured spreadsheets. Ganesan posited password management solutions could provide a middle ground between sensitive systems access and potential data breaches. The password system provides a level of security and provides a technological scan of all Active Directory linked systems for security (Ganesan, 2016).

The weak point for password-protected systems is the hardcoded default passwords for the enterprise. Hackers gain access to the default password script; they may be able to decode and wreak havoc on the network (Ganesan, 2016). Ganesan (2016) found that web browsers and websites requiring passwords do not have accountability or trace features on information sharing, among others (human vulnerability).

In summary, PCI-DSS guidelines provide business leaders with minimum-security suggestions for the prevention of data breach and or payment-card fraud detection. The PCI-DSS recommendations for card acceptors included information for data retention, password strengths, network security protocols, and on-line card acceptance rules and regulations for data encryption. Rees (2014) stated that the implementation of data-security does not have to be expensive or complicated. The PCI-DSS guidelines best implementation uses QSAs with broad knowledge in the PCI-DSS implementations. The challenge for any QSA or business comes from securing customer's data and card information.

Data Breach

Since the advent of e-commerce web sites, data breaches, and identity theft have increased (Hoffman, 2013). Small (2014) discussed the risk factors and the vulnerability to data breaches. The server is the most vulnerable location for a data breach to occur (Small, 2014). Although the server is vulnerable, the end-user and or the cardholder have responsibility for ensuring data safety.

Data-security includes end-users changing passwords and cardholders, ensuring their cards are safe and secure when not in use (Gold, 2014). Breach containment involves identifying the problem and performing the necessary steps to stop the discovered breach (Gold, 2014; Small, 2014). To evaluate risk, security specialists should determine if a data breach has compromised the system or data, and then they must estimate costs for breach cleanup.

Leaders must notify customers of the breach and any payment-card users of the potential for fraud activity on the customers' cards (Small, 2014). In addition to the reactive steps, leaders must take proactive steps to prepare for potential future data breaches through updated spyware, phishing programs, and anti-virus software (Gold, 2014; Small, 2014). Hardware personnel must inspect card readers for potential problems.

The POS breaches at major retailers such as Home Depot and Target involved data breaches caused by BlackPOS malware, enabling fraudsters to collect more than 70 million payment-card numbers (Caldwell, 2014). BlackPOS malware spread incrementally through the POS systems collecting customer data. Caldwell (2014) indicated that TrendMicro's POS anti-malware software was not working fast enough to detect the Trojan. Caldwell stated the anti-malware and anti-virus software on the Target POS system detection failed and caused the data breach at Target.

Caldwell (2014) suggested if the malware and anti-virus servers worked at maximum speed, the potential for trapping and cleaning the malware would increase and

decrease the effect of the infection. Caldwell suggested that POS system administrators should remotely shut down the terminal and reimage the machine after intrusion detection to eliminate additional infections. Caldwell's research focused on Europay, MasterCard, and Visa (EMV) chip and pin technology.

Card issuers expect to see a reduction in data breaches because of increased security. Caldwell (2014) posited mag-stripe technology is attractive to fraudsters because of the ease of cloning payment cards. Chip and pin are harder to clone and is less attractive to fraudsters (Caldwell, 2014). EMV technology has become a global standard for payment-card issuers (Caldwell, 2014). EMV, or chip and pin technology, uses a microchip technology at the acceptor's checkout location.

Caldwell (2014) stated throughout the transaction process, EMV transactions use encryption. The EMV card machine may use the mag-stripe if the merchant uses the tampered with chip Ireader (Caldwell, 2014). Mag-stripe cards are susceptible to cloning, which enables criminals to obtain customer data. Card acceptors' equipment needs upgrading to read the new chip and pin cards, which the card companies' issue (Caldwell, 2014). After 2 years of equipment and software upgrades, some small retailers are not accepting chip cards because of the cost of new card-reading equipment.

In summary, data breaches attack the server, which is the most vulnerable location in the network for card transactions (Gold, 2014; Small, 2014). The server vulnerability to malware and virus attacks leave card acceptors and data-security personnel to create new security policies for network access and card fraud detection (Small, 2014). The

advent of the chip and signature card has reduced brick and mortar card fraud; online card fraud continues to increase because of card-not-present (Caldwell, 2014).

Dark Web

The dark web or deep web contains content that has not been indexed by popular search engines like Google or Yahoo (Finklea, 2017). Finklea (2017) posited that the dark web is used for both legal and illegal activities. The legal activities, as described by Finklea, include Intranet sites at businesses and government installations. Illegal activities involve identity theft, payment card information theft, and disrupting supply chains (Finklea, 2017; Wilson, 2019).

Supply chain disruption occurs when a person or persons launch ransomware or malware attacks (Wilson, 2019). Ransomware (software) attack attacks a computer and demands the person or organization to pay a ransom to release the files (Cabaj, Gregorczyk, & Mazurczyk, 2018). The payment may be in bitcoin or a request for the local country's currency (Bancroft & Reid, 2016). The victim of the ransom does not have to pay the ransom to have the files released. The victim may reset their computer system to a time before the attack.

The dark web relies on anonymity (Bancroft & Reid, 2016). The anonymity of the users and the servers conceal the illicit activity. The original idea for the dark web created by the United States Navy was for open lines of communications (Bancroft & Reid, 2016). However, as the web developed with more layers, criminals and others discovered the dark web became a communication avenue without fear of persecution.

Although the dark web has multiple uses for illegal activities, fraudsters can buy and sell information. The victim's personal information is broken down into name, address, social security number, card numbers, and income brackets (Finklea, 2017). The fraudster can sell each data cell (Finklea, 2017). The sale of personal information provides the opportunity for identity theft and payment card fraud.

Payment-Card Fraud Detection

Fraud is an unauthorized activity-taking place in electronic payment systems (Vaishali, 2014). Card processors and issuers work together using various detection techniques (Gold, 2014). The techniques involve software and physical card traits (Gold, 2014). Additionally, Gold (2014) described the shift in card usage from credit to debit cards as one of the results of card fraud. Europe was one of the first areas to issue prepaid debit cards using chip and pin technology (Gold, 2014). Gold explained chip and pin technology employed in Europe reduced card fraud. However, thieves can still emulate the card and obtain a falsified chip (Gold, 2014).

The attacks on smart cards with chip and pin technology forced Visa and MasterCard to enable chip and pin payment architecture in support of encrypted storage of the four-character PIN on the card (Gold, 2014). Gold (2014) revealed how a retailer's PIN reader might be hacked to view the POS system. Retailer's point of sale (POS) systems are vulnerable to attack by malware. Malware has the capability of disabling the POS system's chip and pin reader and forcing the mag-stripe reader into use (Caldwell,

2014; Gold, 2014). Malware or RAM scraper software exploits the data from the retailer's POS terminal and transmits it back to the hacker's computer (Caldwell, 2014). Manworren, Letwat, and Daily (2016) described how malware attaches to customer data and transmits back to hackers. The malware process captures the customer's card information and stores the information on the commandeered server (Manworren et al., 2016). Manworren et al. examined how secure Target's security analysts considered the network.

Plachkinova and Maurer (2018) posited that the Target network is technologically a leader in the industry with security. The Target system had one flaw: third-party contractors' logins did not have the appropriate rights to block the person(s) out of the payment-card system (Manworren et al., 2016). Malware introduction came through the contractor's access to hack the Target system (Manworren et al., 2016). The malware attack allowed hackers to obtain millions of customers' information before analysts realized the infection (Plachkinova & Maurer, 2018). The lack of responding to malware notifications cost Target Corporation, both its reputation and customers (Manworren et al., 2016).

Card acceptors and system administrators tend not to keep up with security patches and anti-virus software updates (Small, 2014). The lack of applied security patches to the operating system or other installed software either enables unauthorized access to the network through malware or means (Manworren et al., 2016). Small (2014) also discussed the need for changing people's perception of information security, creating

data stewardship, educating, teaching, and mentoring. Small also discussed the need for rewarding those individuals who are data-security conscious and sanction those people who break the data-security rules.

Payment-card fraud detection systems and methodologies vary widely between banks, card processors, and retailers. Data-security analysts need to be prepared for data breaches and should have a plan in place for security breaches. Malware and phishing programs open the door for potential data breaches. The data collected in a breach provide information about customers' and customers' card numbers. Fraudsters and or hackers obtaining the information may open new accounts in an unsuspecting person's name and ruin that person's credit. The success or failure of the IT department depends upon security policies and procedures. Collectively, safety is every employee's responsibility. IT security should be about flexibility, not rigidity (Khanna, 2013).

Dal Pozzolo, Caelen, Le Borgne, Waterschoot, and Bontempi (2014) discussed the current systems technology for detecting fraudulent financial transactions using fraud management in financial data streams. The application's use allows for policy constructs created by human programmers (Dal Pozzolo et al., 2014). Fraud-detection software evaluation allows for a comparison of the old system with potential new software (Dal Pozzolo et al., 2014). Dal Pozzolo et al. introduced a hybrid-fraud detection model for e-commerce and payment-card fraud. The hybrid detection model demonstrates an increased detection of allowed connections and charges and decreased fraud instances (Dal Pozzolo et al., 2014).

West and Bhattacharya (2016) discussed various fraud detection systems. West and Bhattacharya focused on computational intelligence (CI) and data mining methods for detecting financial fraud. CI includes logistic regression analysis, neural networks, and support vector machines (West & Bhattacharya, 2016). West and Bhattacharya used three standards for determining the performance of each method: accuracy, sensitivity, and specificity. Accuracy measures the ratio of successfully detected fraud transactions compared to unsuccessful detection.

Sensitivity compares the number of items correctly identified as a fraud in comparison to false positives. Specificity refers to the same concepts for legitimate transactions (West & Bhattacharya, 2016). Fraud detection is generally viewed as a data mining classification problem, where the objective is to determine if the transaction is fraudulent or legitimate. Fraud detection involves monitoring user behavior using the software to detect fraudulent activity effectively.

Consequences of Payment Card Fraud and Data Breaches

Fraud detection software helps data security analysts and card security analysts to determine if transactions are fraudulent. Consequences of fraudulent transactions may lead to consumer embarrassment for purchases. Businesses such as Home Depot, Yahoo, and Target face similar embarrassment but on a larger scale. Businesses face lawsuits, financial losses, and congressional actions (West & Bhattacharya, 2016; Whitler & Farris, 2017). Consequences for commercial organizations vary by state. Home Depot, for example, governed by the states of Georgia, Indiana, and California, faced United

States congressional actions (Bergman, 2015; Manion, 2015). Sanctions by federal, state, and local laws determine stock prices, consumer trust, and vendor trust. The fallout from data breaches and fraud for consumers and businesses are economic hardships and less access to credit.

Although creditworthiness is one outcome, loss of trust and reputation play a significant role in public opinion. Trust is a fundamental or crucial element (Simon & Cagle, 2017) for corporations, governments, and individuals. Simon and Cagle (2017) defined reputation as the amount of regard that stakeholders and consumers place in a company. Reputation plays a primary role in customer satisfaction for the business (Bergman, 2015; Simon & Cagle, 2017). An organization that loses both trust and reputation may not survive the publicized negative information.

The negative effect of consumer notifications of a data breach has led the way for the United States Congress to develop new requirements for cybersecurity (Bergman, 2015). Congressional leaders are focusing on requirements for full disclosures and responsible disclosures for data breaches and the effect on the consumer market (Bergman, 2015). These are just a few of the consequences' consumers and businesses alike face when data breaches and card fraud occur.

Payment-Card Fraud Elimination Models (Software)

Payment-card fraud elimination models used through 2019 provide a background understanding of the models used by a business. Researchers have offered a variety of potential solutions to payment-card fraud. Additionally, banks and card processors

developed methodologies to detect card fraud (West & Bhattacharya, 2016). The methodologies discussed included (a) support vector machines, (b) decision tree algorithms, and (c) hidden Markov models to suggest a few (West & Bhattacharya, 2016). Organizational leaders may use a mix of human and software and or hardware to detect fraudulent usage. The mix of human and software detection processes fail due to human error (West & Bhattacharya, 2016).

Clustering. X-Means clustering models detect an unsupervised learning algorithm, which solves a well-known clustering model (Chang & Chang, 2014). The statistical study performed by J.-S. Chang and Chang (2014) focused on fraudulent behavior to determine status transitions. J.-S. Chang and Chang identified four fraudulent behavioral means to determine different fraud schemes. The fraud schemes identified by J.-S. Chang and Chang described (a) direct attacks, (b) quick profit, (c) luxury purchases, and (d) price varied purchases. J.-S. Chang and Chang used multiple statistical methods to determine fraudulent transactions.

Direct attack or aggressive fraudsters apply straight tricks to obtain higher ratings within the hacker community (Chang & Chang, 2014). J.-S. Chang and Chang (2014) posited quick profit fraudsters are the classical person looking to make a quick monetary gain. Luxury purchase fraudsters only pay attention to the high dollar items such as artwork or high-end vehicles (Chang & Chang, 2014). The price varied fraud described by J.-S. Chang and Chang involve low price quick move items that most consumers do not notice.

The quantitative methods discussed by J.-S. Chang and Chang (2014) included X-means algorithms (a variance of *K*-means). The X-means cluster development automatically calculates the number of clusters to fit the data set. The X-means formula as applied by J.-S. Chang and Chang traced fraudulent behavior to determine the appropriate fraud profile of the fraudsters. Card fraudsters do not always rely on their initial behavior (Chang & Chang, 2014) because a fraudster changes their behavior to avoid detection.

Vaishali (2014) offered *K*-means clustering as one potential way to eliminate payment-card fraud. Vaishali described hierarchical agglomerative methods [two groups of clusters determining bottom-up data], partitioning methods [data grouping related to data mining], single link method [merging two small like data groups]. Additionally, the methods Vaishali described include the complete link method [merging sets of data], and group average method [compromise of single and complete link methods]. *K*-means is an unsupervised technique for data mining.

The unsupervised technique is useful when there is no prior knowledge about the observation (Vaishali, 2014). *K*-means is a straightforward and efficient method for clustering data. *K*-Means clustering is popular because of (a) ease of implementation; (b) versatile implementation, functionality, and termination criteria; (c) time complexity and storage; and (d) random data shuffling (Vaishali, 2014).

Vaishali (2014) stated that fraud could not have 100% detection using the *K*-means method. The plan identifies safe transactions as fraud and fraud transactions as

safe transactions. The additional problematic area addressed is the lack of available data due to confidentiality issues that give little chance to share real data sets and assess existing techniques. Vaishali discussed several learning methods for payment-card fraud detection systems, methods including statistical models, static approaches, and K-means. The results are not always accurate as payment cardholders spending patterns dictate the use of the algorithms (Vaishali, 2014).

Clustering is not always an accurate algorithm to detect payment-card fraud. X-means (K-means variant) works with the dataset to determine card fraud. K-means is an unsupervised method of determining card fraud. The card-fraud predictions used by clustering methodologies may provide false positives for fraud transactions based on the customer's usage patterns.

Neural networks. Neural networks are popular with business leaders for payment-card fraud detection (Halvaiee & Akbari, 2014). Neural networks consist of a set of artificial neurons. The neural network mimics the human brain through customer spending pattern recognition (Halvaiee & Akbari, 2014). The neural network has the capability of predicting future values or events based on customer card usage.

Halvaiee and Akbari (2014) posited current fraud detection methods that are using signatures as time-consuming. Mobile fraud, according to Halvaiee and Akbari, uses artificial neural networks. Artificial neural networks predict card users' behavior and compare the usage to current usage behavior patterns. Halvaiee and Akbari posited

payment-card fraud detection requires a high rate of transaction detection while keeping false alarm rates low.

Van Vlasselaer et al. (2015) discussed a different approach to the use of neural networks to detect card fraud. The approach Van Vlasselaer et al. discussed involved the use of time-stamped, labeled transactions, and machine-learned transaction history for fraud detection. The time-stamped transactions use a sliding window of time to determine non-fraudulent charges. Van Vlasselaer et al. time windows include short term, medium, and or long-term, and customer transaction history. The proposed method uses real-time card transactions.

The approach Van Vlasselaer et al. (2015) incorporated combines both real-time and network-based attributes. The approach uses the regency-frequency-monetary value (RFM) network (Van Vlasselaer et al., 2015) using the cardholder's past transaction history. A regency-frequency-monetary value network approach to fraud detection uses a time range for the transaction, usage frequency, and dollar amounts spent on the card. Regency-frequency-monetary value, according to Van Vlasselaer et al., also used geographical data and demographic information for determining transaction normalcy.

In summary, neural networks learn to capture and represent complex relationships using cardholder's past transactions. Neural networks represent the human brain through artificial intelligence and the ability to learn. The advantage of neural networks is the ability to represent linear and nonlinear relationships from the data model.

Artificial intelligence. Halvaiee and Akbari (2014) reviewed the use of artificial intelligence (AI) to determine payment-card fraud. AI's design operates similarly to the human brain. Halvaiee and Akbari stated that the AI system detects fraud by using record processes and determines adverse transaction records using customer-spending patterns.

Halvaiee and Akbari (2014) focused on the Artificial Immune Recognition System (AIRS), a classification algorithm system. AIRS features include self-regulation, performance, generalization, and parameter adjustment. Halvaiee and Akbari described AIRS using generalization through data reduction to increase the detection of fraud transactions.

Halvaiee and Akbari (2014) posited AIRS knows the cardholders' spending patterns and determines the difference between right and fraudulent transactions. AIRS detects and learns new methods of misuse using the customer's payment-card usage. The system acts as the human body in detecting viral spending conditions and fighting off those questionable spending habits (Halvaiee & Akbari, 2014) that are multiple charges in a brief period at the same merchant.

West and Bhattacharya (2016) performed a data mining study of artificial intelligence to detect payment-card fraud. The data mining process used visualization methodology to present clear and understandable observation results (West & Bhattacharya, 2016). West and Bhattacharya posited the rules for the system classifies

data into understandable formats for the human mind to grasp. The rule should capture fraudulent transactions; however, no system is infallible (West & Bhattacharya, 2016).

West and Bhattacharya (2016) posited the problems with the rule-based system are the test data sets based on actual data; the problem is incurred when the system has already learned the customer's spending habits. The focus of the study covered detection methods (a) data mining, (b) performance metrics, and (c) algorithms. Performance metrics assisted Jarrod et al., with a quantitative study to balance the positive and negative ratios (West & Bhattacharya, 2016).

Artificial intelligence uses the same process as neural networks. AI systems trap the positive and negative attributes, using algorithms as previously demonstrated. The problems encountered by West and Bhattacharya (2016) involved the test data set as a live data set. West and Bhattacharya stated the metrics for fraud determination systems need to use live data to determine if the transactions flagged are good or bad.

M.A.S.T. Rosaci and Sarne (2014) discussed how e-Commerce plays a role in online shopping and card-not-present fraud transactions. The technology used for social media commerce and e-Commerce sites, including local brick and mortar merchants with websites, use similar fraud detection models. Rosaci and Sarne discussed the aspects of e-commerce (EC) playing a pivotal role in card not present shopping on the web. The transactions described by Rosaci and Sarne are Business to Customer (B2C). The technology allows the customer to enter his or her card number into a website to purchase

goods or services. The customer may not know if the page is fraudulent, as the page may look legitimate.

Rosaci and Sarne (2014) described the need for payment-card-not-present security using multi-agent technology. The potential fraud detection system supports several aspects of Business-to-Customer EC activities (Rosaci & Sarne, 2014). A multi-agent system for traders (M.A.S.T.) detects fraud transactions through a personalized approach. M.A.S.T. is a set of XML-based personal agents designed to assist the customer and business in managing personal consumer profiles.

The e-payment model avoids transferring sensitive data through the reinforcement of trust between merchants and customers (Rosaci & Sarne, 2014). The standards allowed by PCI-DSS do not have a set time to expire the card information (Rosaci & Sarne, 2014). However, to increase customer information security, M.A.S.T. offers the card acceptor a reduced time for data to live for payment-card authorization (Rosaci & Sarne, 2014).

M.A.S.T. uses XML protocols providing sensitive data to the acceptor and the financial institution to approve or deny the transaction. M.A.S.T. agents build, update, and exploit user information to offer customer orientations by weighting shopping habits. M.A.S.T. needs additional tweaking to improve performance and reliability. M.A.S.T. is coded software with the potential for malware attacks (Rosaci & Sarne, 2014).

Although payment-card fraud and identity theft occur in multiple ways, card issuers, processors, and acceptors implemented quantitative or algorithmic solutions.

Additional solutions card approvers and acceptors have implemented computer hardware such as Cisco firewalls, and vector decision machines (Rosaci & Sarne, 2014). Card acceptors and processors in 2015 and prior years have used quantitative and algorithmic software solutions with little result in a reduction of fraudulent transactions (Rosaci & Sarne, 2014). Sahin et al. (2013) offered a quantitative software method for deciding if transactions are fraudulent.

Sahin et al. (2013) discussed the bias in selecting new fraud detection systems by comparing the old and new systems. The old systems have the customer data, and spending habits established, and the new system would need to *learn* the customer's habits. The bias arises from the fact that the old system would terminate the transaction account when fraud would occur, but the proposed new system would not learn the customers' spending habits. Sahin et al. performed a statistical study to determine the acceptability of the proposed new system(s).

Sahin et al. (2013) discussed how the determination process involved that the biases of the multinomial estimators. The lower the ratio, the less likely the transaction may be fraudulent (Sahin et al., 2013). The probabilities discussed by Sahin et al. include costs to the business and the consumer. The costs to the firm may not be apparent to the bank or the consumer when a fraudulent transaction is detected (Sahin et al., 2013).

Different definitions apply to the costs of doing business; such definitions include recovery costs to both parties involved. Sahin et al. (2013) discussed fraud as a documented problem in a wide range of fields. In summarization, a multi-agent system

for traders relies on artificial decision-making. Multi-agent systems offer reinforced learning mechanisms. The mechanisms used to motivate people to address issues involved in the techniques for machine learning.

Hidden Markov model. Mishra, Panda, and Mishra (2013), and Vojir, Matas, and Noskova (2016) described the hidden Markov model as a finite set of states linked by a probability distribution. Mishra et al. stated the distributions control the set of probabilities called transition probabilities. State-dependent determines the outcome or observation generated by a probability distribution. Mishra et al. described the outcome as only visible to an external observer and, therefore, the hidden states.

Ekinci, Lentin, Uray, and Ulengin (2014) and Vojir et al. (2016) described the hidden Markov model to detect fraudulent payment-card transactions. The model uses algorithms to detect fraud. The algorithms learn the consumers' purchasing habits, calculate the probability, and constructs training sequences. The detection phase generates observation symbols, form new sequences by adding to existing sequences, calculates the probability differences and tests if both are the, same the transaction equals normal else the transaction equals fraud.

Van Vlasselaer et al. (2015) indicated that security is one key area where researchers are focusing on their studies. Van Vlasselaer et al. posited that network - intrusion detection systems attempt to detect attacks through network and analysis of the information from various areas to identify intrusions. Cardholder's usage patterns determine intrusion (false usage) or if an acceptable cardholder transaction. The patterns

indicate to the issuer how the person uses his or her card. The hidden Markov model is an anomalous detection system. Van Vlasselaer et al. stated that usage patterns help issuers develop immune systems to attack.

Payment-card processing using mobile technology opens the door for criminalistic activity, according to Yelland (2013). Ortiz-Yepes' (2014) cell phone technology uses Near Field Communication (NFC) to transmit card information between the acceptor, processor, and the bank and back to the acceptor. NFC technology has a significant flaw concerning data transmission between the card and the phone. The smartphone link allows fraudsters the capability to connect to the phone and obtain the data through wireless transmissions (Ortiz-Yepes, 2014).

Yelland (2013) discussed how fraudsters hack cell phone service because of mobile phone security weaknesses. One-way Yelland discussed was for 3-way calls multiplying into multiple calls from the originating phone to one of the high-cost phone services for international calls. Ortiz-Yepes (2014) identified Near Field Communication (NFC) technology for mobile to accept payment cards. NFC routes card information via a contactless card terminal application.

Cagalj, Perkovic, Bugarcic, and Li (2015) supported smartphone technology as continuously evolving. The newer cell phones come programmed with Near Field Communication (NFC). Cagalj et al. explained that smartphone usage included financial transactions through mobile banking applications. The applications are vulnerable to *mafia fraud attacks*.

Cagalj et al. (2015) explained *mafia fraud attacks* using the example of a folded piece of paper (*fortune cookie*) to capture the unsuspecting cardholder's data. Cagalj et al. stated that the criminal uses the unrelayed transmission information to trap the data provided by the smartphone user when using NFC transactions. Cagalj et al.'s report portray to the reader transaction timing and potential areas for data capture by criminals. Cagalj et al. defined one process to delay transaction times to reduce fraud by using *force*.

Halvaiee and Akbari (2014) discussed using AI to determine payment-card fraud. The study focused on increased detection speed 25% more than current AI speeds. Artificial Immune Systems (AIS) model immolates the human immune system. AIS detect fraud using record processes and determine adverse record methods (Halvaiee & Akbari, 2014). Halvaiee and Akbari reported how the AIS system recognizes the cardholder's spending patterns by determining the difference between good and lousy card transactions. AIS detects and learns new methods of payment-card misuse. The system acts as the human body in detecting viral conditions and fighting off those conditions (Halvaiee & Akbari, 2014).

Potential 2015 and earlier payment fraud-detection systems used multiple types of processing equipment and algorithms. Gold (2014) and Wolf et al. (2015) provided a definition of supervised machine learning for card fraud detection. Carneiro, Figueira, and Costa (2017) discussed the supervised machine learning system for detecting credit card fraud. The supervised machine characterizes the card user's spending habits

(profile). Carneiro et al. study offered the reader information on support vector machine (SVM) model usage of multiple kernels involvement that includes several fields of user profile information instead of spending habits.

The simulation used by Gold (2014) and Wolf et al. (2015) indicated improvement in the actual identification of fraud. Gold and Wolf et al.'s test data showed decreases in false positive and false negative identification of fraud charges. Gold and Wolf et al. used three different fraud probabilities: Quadratic, linear, and RBF, from 0.30 to 0.50, changing the data size from 30 to 100. The RBF kernel outperformed the linear and quadratic kernel in all fields.

Gold (2014) and Wolf et al. (2015) concluded that machine learning algorithms were able to detect the user to root attack categories significantly. Gold and Wolf et al. stated no procedure devised for kernel delimitation to obtain the best kernel functions. The study opened the door to additional research areas using different classifiers for the SVM. The information presented by Carneiro et al. (2017) provided the foundation for the potential solution to credit-card fraud detection systems.

Richhariyva and Singh (2014) evaluated emerging card fraud challenges and resolutions. Richhariyva and Singh found growth in fraud sophistication and scope paralleled improvements in detection systems. New fraud detection systems are costly, as card fraud continues to rise; the progress to stay ahead of fraudsters continues to lag (Richhariyva & Singh, 2014).

Richhariyva and Singh (2014) posited the growth in card fraud continues, and banks and other issuers need to stay ahead of the curve. Technology and enterprise-oriented data-security analysts work on user and enterprise profiles, branding, outliers, and internal controls to ensure customer resolution to data breaches (Richhariyva & Singh, 2014). Seeja and Zareapoor (2014) recommended an intelligent card-fraud detection system.

The hidden Markov model (HMM) is scalable to large transaction data sets and processes transactions faster. The HMM uses cardholders' usage habits to apply the knowledge learned to determine if the transactions are fraudulent or correct. Dal Pozzolo et al. (2014) discussed software systems technology for detecting fraudulent financial transactions using fraud management in financial data streams. The application's use allows for policy constructs created by human programmers (Dal Pozzolo et al., 2014).

Fraud-detection software evaluation, as discussed by Dal Pozzolo et al. (2014), allows for a comparison of the old system with potential new software. Dal Pozzolo et al. introduced a hybrid-fraud detection model for EC and payment-card fraud. The hybrid detection model demonstrates an increased detection of allowed connections and charges and decreased fraud instances (Dal Pozzolo et al., 2014).

West and Bhattacharya (2016) focused on CI and data mining methods for detecting financial fraud. CI includes logistic regression analysis, neural networks, and support vector machines (West & Bhattacharya, 2016). West and Bhattacharya used

three standards for determining the performance of each method: accuracy, sensitivity, and specificity.

Bhatia, Bajaj, and Hazari (2016) and Kabir, Onik, and Samad (2017) analyzed payment-card fraud detection using different techniques: HMM, neural networks, Bayesian learning, support vector machines, K-nearest neighbor, and Dempster Shafer theory. Bhatia et al. performed a fusion approach to Dempster Shafer using Bayesian learning. The process fuses cardholder usage and Bayesian learning.

The process combines predetermined suspicion levels and actual patterns to determine if the transaction is legitimate (Bhatia et al. 2016). The process, as described by Bhatia et al. (2016) and Kabir et al. (2017), is highly accurate and quick to process; however, the cost is prohibitive, and processing speed is slow. Card issuers, acceptors, and processors use the processes to determine fraud or stolen identities, card issuers and processors follow PCI-DSS recommendations for Chip and PIN cards.

Chip and PIN Payment Cards

The chip and pin cards use computer chip or smart card technology to improve the card issuer's capability to authenticate a customer's transaction (Sullivan, 2013).

Sullivan (2013) stated that the chip card uses a secure code authentication process known as dynamic data authentication. The chip and pin cards are harder and more expensive to duplicate, additionally, and the chip offers enhanced protection to the cardholder's information (Sullivan, 2013). The chip card generates additional transaction code

sequences for similar computer network users, changing their password at regular intervals (Sullivan, 2013).

F. Wang, Chang, and Lyu (2015) proposed an additional security measure to include a onetime transaction authentication code. The proposed transaction code, per F. Wang et al., deletes itself after the transaction completes as either approved or denied transaction. The introduction of additional security measures introduced by F. Wang et al. uses facial recognition software for consumer and issuer protections.

Sullivan (2013) posited fraudsters who duplicate chip cards use the duplicated card for *card-not-present* transactions. The card information, according to Sullivan, is obtained through phishing and malicious EC site. Transactions made in-person using chip and pin, or a fraudster and pictures may intercept QR coded cards (identifying picture of the cardholder changed to match the person presenting the card (Wang et al., 2015).

Payment-card fraud detection is a costly problem for card acceptors. The cost of false-positive affects the merchant and the bank issuing the card. However, if the processor and the issuer fail to detect the fraud, the transaction cost is lost, the effect to the merchant can be very high (Bahnsen, Aouada, Stojanovic, & Ottersten, 2016). Collectively safety is every employee's responsibility. IT security should be about flexibility, not rigidity (Khanna, 2013).

The plethora of research studies forms the fundamental focus of the study involving the effects of identity theft and data breaches, public perception, and the

organization's reputation. Reviewed literature examined (a) the role of software, (b) fraud detection methodologies, and (c) new technology such as chip cards with limited results in reducing payment-card fraud. The PCI-DSS recommendations offer business leaders and data-security professionals a framework for developing secure networks and transaction processing guidelines (Clapper & Richmond, 2016; Fernandes, 2015).

Payment-card transaction processing follows the PCI-DSS guidelines. Payment-card fraud has multiple software algorithms available for detecting fraud such as Markov Model, Fischer Algorithm, and artificial intelligence packages (Gold, 2014; Manworren et al., 2016). The results of the review lead to conclusive arguments for the urgent need to explore anti-fraud strategies to minimize the rising trend of payment-card fraud and identity theft, among other challenges of network security, transaction processing, and card issuers struggles to develop processes for identifying fraudulent transactions.

Transition

Section 1 contained a discussion on the need to investigate payment-card fraud and avenues for reducing or eliminating fraud. The focus of the research problem is on payment-card fraud and identity theft. United States Government Accountability Office (2014) posited data breaches increased for banks and governmental agencies to 255,666 in 2013. A background discussion provided information about data breaches, payment-card fraud, and identity theft in the United States retail arena. Little research is available about the influence of fraud prevention elimination (Jha & Westland, 2013).

This section also contains a discussion of the purpose of the research study, along with the research method, the nature of the study, the geographic location of the study, and literary review. The literary analysis included the evolution of payment-card fraud, identity theft, and data breaches. Also discussed are the current fraud detection and data breach methodologies.

The literature review also involved reviewing data on retail payment-card and global card fraud systems. Section 1 included a discussion of the assumptions, limitations, and delimitations of the study. Section 2 contains the details of the project, such as the role of the researcher, participants, data collection method, population and sampling, research method, and design. Section 3 includes the findings of the study. Additionally, Section 3 covers the implication of social change and recommendations for action and further research.

Section 2: The Project

In Section 2, the role of the researcher is defined; the purpose of the research is described, the approach and criteria for selecting prospective study participants are outlined. Also, in this section will be a brief examination of research methods, study design methodologies, and the rationale for selecting a qualitative method with multiple case design for this study. Also covered are the considerations for ethical parameters and principals applicable to this study. In addition, the section contains the outline of population sampling, followed by a review of the methods for collecting, organizing, and analyzing the study data. Section 2 concludes with a discussion of the approach to ensure the reliability and validity of the research and steps for minimizing potential biases and assuring credibility and confirmability of the study.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies international card processing organizations use to minimize payment-card fraud. The targeted population was five to eight data security specialists working for an international card processing organization in the southeast United States who have successfully prevented data breaches and payment-card fraud. The implication for positive social change included the potential for lowering the number of data breaches and payment-card fraud instances, which could provide customers with confidence in using their payment cards, reduce fraud losses, and thereby improve the economy.

Role of the Researcher

The role of the researcher included selecting participants, collecting data, and interviewing participants. Additional goals were to compile, adapt, and translate the data and publicize the results. Other goals included compiling and analyzing data for themes from the data and presenting the findings in Section 3. As a qualitative researcher, establishing connections with the participants ensured the participants' trust and comfort during the interviews.

The choice to research payment-card fraud elimination involved personal experience with data-breaches and payment-card fraud activities encountered at various retail outlets. The type of card fraud I experienced involved my debit card being hacked at a local restaurant. I learned of the fraud when I attempted to use my card for a purchase and my card was no longer active. I am passionate about understanding organization strategies for eliminating and reducing card fraud.

Moustakas (1994) posited the researcher and participants in a case study become one through the processes of epoch, reduction, and imaginative variation. Moustakas indicated that in the quest for new knowledge, the researcher must set aside prejudices. The purpose of the process, known as epoche (Moustakas, 1994), is for researchers to set aside prejudices and biases to ensure pure research. As the researcher, I eliminated personal bias by suspending judgment and accepting the information as presented by the participants.

Applebaum (2014) recommended that researchers use a journal to track all study-related actions to reduce the potential for biases. Moustakas (1994) discussed how a researcher's full accounting of firsthand experiences in a topic leads to transparency in the overall validity of the study. Annotated notes were made on the experience of the participants with the topic under study as part of the exploration of the phenomenon using an electronic journal such as OneNote by Microsoft.

Clarity and competence are encouraged in conversation without influencing the answer or outcome (Shaw & Erren, 2015). The modules concerning ethical research by the U.S. Department of Health and Human Services' (1979) *Belmont Report* guidelines for using human subjects was completed successfully. The Belmont Report provided the researcher with the participants' fundamental rights and principals identified by the U.S. Department of Health Human Services (HHS) commission (Friesen, Kerns, Redman, & Caplan, 2017; Rogers & Lange, 2013).

The Belmont Report commissioners described the guidelines and principals to assure compliance with HHS guidelines (Friesen et al., 2017; Rogers & Lange, 2013). The guidelines provide specific protections for human subjects' research and include considerations for vulnerable individuals, populations, or groups (Rogers & Lange, 2013). The Belmont Commission provides guidelines for ethics, research principles, and considerations researchers should be aware of when performing research (Rogers & Lange, 2013).

To ensure that the guidelines of the *Belmont Report* (U.S. Department of Health and Human Services, 1979) were followed, each participant signed a consent form, indicating the person's participation was entirely voluntary. Each participant was ethically treated and followed Walden IRB's requirements and U.S. federal regulations. A Walden representative and the vice-president of the international card processing organization signed a DBA Research Agreement, which defined the responsibility of each organization. Each participant signed a participation consent form.

In this study, I served in the role of the primary data collection instrument. I interviewed senior management and data security analysts from my client international card processing organization located in the southeastern United States. The role of researchers in qualitative case studies consists of observing participant behavior and collecting data (Merriam, 2015; Yin, 2014). A researcher's role includes observation, taking field notes, collecting data, and guiding the participants through the interview process and maintaining objectivity during data collection (Marshall & Rossman, 2016).

Abiding by the HHS guidelines ensures the ethical treatment of participants. The guidelines provide the basis for protecting individuals from harm and secure their well-being (Dudley et al., 2015). Fair treatment of the interviewees included allowing for age, experiences, deprivation, competence, merit, and position. I ensured the interviewees understood and that I had their (signed) consent. I included a formal cover letter of introduction (see Appendix C) and consent form (see Appendix D) in the appendix section.

I chose to use an investigative interview protocol (see Appendix F). The information contained in the interview protocol served as a guide to interview participants with the same standards regarding reliability and validity (Jacob & Furgerson, 2012). The investigative protocol allowed the interviewees the option of open-ended free recall questions (Benia, Hauck-Filho, Dillenburg, & Stein, 2015). Benia et al. (2015) posited that after exhausting open-ended questions, the interviewer has the option to ask option-posing questions to gain further clarification. The interviewees' responses to the questions tend to be more informative and more accurate responses to focused questions. The open-ended questions allowed the interviewer to probe further, allowing the interviewee the opportunity to provide additional details (Benia et al., 2015).

Participants

DeFeo (2013) stated that qualitative researchers should identify professionals who have comprehensive knowledge in a specific social or cultural knowledge area. DeFeo described the optimal standard to conscribe skilled persons to implement a saturation level of knowledge about the intended research topic. Calderoni, Brunetto, and Piccardi (2016) recorded that qualitative researchers affirm the strategy of selecting interview candidates who are appropriate for the direction of the study. The importance for me as the researcher was to formulate ideas afforded by the participants without bias. Participants met the following minimum criteria (a) information security specialists, (b) 18 years of age or older, (c) 10 years' experience, and (d) works for an international payment-card processing company headquartered in Georgia.

Researchers can use various strategies to contact prospective companies (Reilly, 2013). Contacting organizational leaders in-person or by phone is an effective way to ask for permission to collect data from a business (Bell, Bryman, & Harley, 2015). Visiting prospective organizations and contacting them by e-mail are effective strategies because researchers can provide sufficient information about the study to the business leaders to make a decision (Gandy, 2014). Before meeting potential participants, I included a letter of introduction through e-mail to explain the study focus and ensure the privacy of the participants, the collection of signed consent forms, and my handling of concerns and questions. I used purposive and snowball sampling to identify five to eight participants.

Calderoni et al. (2016) suggested that researchers meet potential participants before the interview process to assist the researcher in establishing a meaningful working relationship with participants. Therefore, I contacted senior managers of the international payment-card processing organization in Georgia. The participants had at least 10 years' experience, with a minimum of a bachelor's degree. I contacted the participants using e-mail and in-person to request permission to collect data. Calderoni et al. recorded that smaller sample sizes provide increased data richness in case studies.

Establishing working relationships with participants required the researcher to build trust, credibility, and rapport (McDermid, Peters, Jackson, & Daly, 2014). To establish rapport with the participants, I met with the participants at a local coffee shop, restaurant, or other location where the participant felt comfortable discussing business strategies. The person's demeanor and daily job-related stress should be considered

during the interview process to prevent upsetting the participant or causing the person's health-related stress (Khanna, 2013).

I considered timing and location to enhance rapport with the participant. To enhance the reliability and validity of the information, Kaiser (2013), recommended withholding the names and other contact information sought through personal contacts at the international payment-card processing company and snowball sampling to provide anonymity. The personal contacts included those persons working in data-security, who met the criteria outlined in the study (Marshall & Rossman, 2016; Yin, 2014).

Research Method and Design

The information provided in the research and design method provided the foundation for gathering the data and guided the focus of the study to answer the primary research question. The researcher may use one or more research methods. The methods available to the researcher are (a) qualitative, (b) quantitative, and (c) mixed methods (Zohrabi, 2013). The research method chosen for this study of reducing payment-card fraud was qualitative.

Qualitative researchers collect data by exploring documents, observing, and interviewing interview participants (Marshall et al., 2013). Kerwin-Boudreau and Butler-Kisber (2016) discussed qualitative research as descriptive methods using exploration, explanation, and presentation of results about a phenomenon as described by the people who experienced it. The focus of this qualitative case study was to explore data-security

analysts' perceptions and experiences for an in-depth exploration of reducing payment-card fraud (Calderoni et al., 2016).

Research Method

Research methods consist of data collection, coding, analysis, and interpretations used by the investigator for their studies. Three conventional methods employed include qualitative, quantitative, and mixed methods (Frels & Onwuegbuzie, 2013; Zohrabi, 2013). The method for this study of reducing payment-card fraud was qualitative because the collection method of data involved emerging questions and strategies.

For the study, qualitative was chosen over quantitative or mixed-method research. A quantitative researcher may target the amount of data, allowing for a broad cross-section and a large volume of numerical data to analyze (Vaitkevicius & Kazokiene, 2013). Quantitative researchers use close-ended questions to test hypotheses and do not allow for additional probing (Vaitkevicius & Kazokiene, 2013). Statistical studies done before 2017 have assisted with creating computer-coding options for payment-card processors and banks, with limited results in catching fraudulent transactions (Dal Pozzolo et al., 2014).

No quantitative methods were used as the purpose of the study was to explore strategies and not test hypotheses. Mixed-method research may enhance the gain made by both methods; however, mixed-method research requires considerable investigative skills and creates additional time and information refining (Venkatesh et al., 2013). Qualitative research may offer more precise insights on payment-card fraud reduction

strategies (Venkatesh et al., 2013; Zohrabi, 2013). Mixed methods research was not appropriate for this study, as there was not a quantitative component necessary for this study.

Research Design

Calderoni et al. (2016) described research design as an action plan that connects theoretical frameworks, research question(s), and the research methodology. A qualitative case study was chosen to explore the experiences of data-security specialists as a means of reducing payment-card fraud. The primary focus of this study was to explore the data-security experts' perceptions and experiences for an in-depth investigation of the primary phenomenon.

Three research designs were considered (a) phenomenology, (b) ethnography, and (c) case study. Phenomenology is appropriate when researchers hope to describe and analyze how individuals interpret their life experiences regarding specific phenomena (Moustakas, 1994). Ethnographic researchers engage with study participants through extensive fieldwork to establish a cultural description (Moustakas, 1994). Neither phenomenology nor ethnography was appropriate for this proposal because the focus was not on the meaning of individual experiences or cultural descriptions but rather on identifying strategies to eliminate credit card fraud.

A qualitative case study design was chosen to analyze the accouterments of events, experiences, activities, and processes on interviewees through multiple information sources over time. Kerwin-Boudreau and Butler-Kisber (2016) described

how researchers use the case study design to triangulate information from multiple sources to derive answers to the research question(s). Researchers and scholars using the case study design explore the experiences of the affected group of people or organizations over a period to gain a better understanding of the contributing factors to the phenomenon (Calderoni et al., 2016).

Case study researchers assist with creating an understanding of complex ideas and analysis of situations (Yin, 2014). Case studies researchers explore specific methods for grasping and understanding investigative information. The researcher may explore a restricted case or may study an exploratory case as described by Yin (2014).

Case study researchers focus on specific contexts and situations over time (Dorrian, Grant, & Banks, 2017). Exploratory case study researchers have little control over events, and the investigation allows for information gathering from more than one source to enhance the validity of the single case study (Miller, 2017). Data saturation relates to the depth of the sample and the ability to find repetition in the information through interviewing most of the employees of a small business (O'Reilly & Parker, 2013). In an exploratory case study design, data saturation occurs when the participants, the ones with the most knowledge, provide no new insights to the investigative topic (O'Reilly & Parker, 2013). The interviews were reviewed in sequence and stopped when the final interview revealed no additional information.

Williamson, Leeming, Lyttle, and Johnson (2015) indicated that researchers rely in part on sample size to achieve *data saturation*, which occurs when no participants

reveal no new information. Data were gathered through semistructured interviews and organizational documents related to the research question. Through methodological triangulation, I corroborated and triangulated the interview data with the secondary data to confirm or disconfirm the statements by the participants. Data saturation occurred when there was no new information gained from the participants and secondary data (Fusch & Ness, 2015).

Population and Sampling

The population for this qualitative case study was a purposive sample of one vice president and three senior data security analysts from an international card processing organization in the southeastern United States. Purposive and snowball sampling techniques were used. Purposive sampling is a type of sampling in which researchers use their judgment in interviewee selection based on the criteria of the investigative study (Barratt, Ferris, & Lenton, 2015). The snowball sampling technique allows the initial interviewees to recommend additional participants (Dusek, Yurova, & Ruppel, 2015). Patton (2015) defined purposeful snowball sampling uses the interviewer's ability to select participants that can add understanding and additional information to the research topic.

The focus of this study was on the perceptions of data-security professionals working for an international payment-card processing company in Atlanta, Georgia, to determine which factors improved data-security to reduce or eliminate payment-card fraud. The targeted interviewees were data-security specialists currently working within

the international payment-card processing company's IT department. The target population in the study were data-security specialists who have common defining characteristics identified for the research.

The sample selection targets a population that possesses data-security specialists characteristics appropriate for the study. According to Lipstein, Brinkman, Sage, Lannon, and DeWitt (2013), the combination of purposeful and snowball sampling involves the selection of participants who have experienced the phenomena under study and who could also address the research problem including the research question. Simple random sampling was not suitable for the study because random sampling enables researchers to address general populations without specific criteria (Griffin, Abdel-Monem, Tomkins, Richardson, & Jorgensen, 2015).

The appropriate number of participants depended upon the nature of the inquiry (O'Reilly & Parker, 2013). According to O. C. Robinson (2014), there is no appropriate number of respondents in a qualitative case study; instead, the researcher stops data collection when participants provided no new information (Huh, Verma, Rayala, & Bobba, 2017). Data collection ceased when four of four participants provided no new relevant information.

Participants were polled to choose a comfortable location for conducting face to face interviews such as coffee shops, on-site conference rooms, or a public place of their choosing (Doody & Noonan, 2013). Interviews were conducted at a location each participant selected (Holmberg & Madsen, 2014). By allowing the participants to select

the interview location, more information may be imparted with fewer feelings of stress and fear of compromising positions (Holmberg & Madsen, 2014; Houghton, Casey, Shaw, & Murphy, 2013). Location selection is purposeful for imparting fruitful discussions and privacy.

Data saturation occurs when no new information or themes emerge from the study participants (Tran, Porcher, Ravaud, & Falissard, 2016). Information was collected from the vice president and the three data security analysts to ensure data saturation. Member checking and methodical triangulation were used to enhance data saturation. Simpson and Quigley (2016) defined member checking as the process of participants reviewing the rough draft of the information presented and refining the information for accuracy. The use of member checking allows the researcher to achieve data saturation, authenticate the data, assure the accuracy of the information imparted through the collected data (Marshall & Rossman, 2016).

Ethical Research

Participants must give informed consent, and researchers must accept ethical responsibility when performing research. Walden University requires informed consent before research with human subjects could begin. The IRB approved research process included a review of the consent forms, letters of cooperation, and interview information. The human subject material had to follow federal guidelines and allow for any unexpected events beyond the researchers' control. Walden University's approval number for this study is #03-22-19-0411663, with an expiration date of March 21, 2020.

Before performing data collection, Walden University IRB approved the study's ethical guidelines. IRB approval protects human research participants' rights (Wolf et al., 2015). The study contained no foreseeable risks or harm to the interviewees, and the participants require no research protection. Participants who met the criteria were invited to participate in the study and receive an informed consent form. Interviewees signed an informed consent form to participate (see Appendix D). Data about the study was sent to the participants via electronic mail and printed hard copies; this allowed the participant to make an informed decision about whether to participate in the investigation.

Participants were informed that they were free to withdraw from the interview process at any time (Marshall & Rossman, 2016). Participants who request to withdraw from the study may do so verbally or in writing without penalty (Palinkas et al., 2015). No incentives were offered for participating in the interviews to avoid coercion and increase the validity of the interviewees' answers. As the researcher, the confidentiality of the participants was ensured following an essential guide to ethical research (Sinha & Yadav, 2017).

The participants received assurances that the records of the study remain private. All interviews were audio-recorded using a digital audio recorder and labeled with the assigned participant code DS01, DS02, through DS4 for the data-security specialists to protect the confidentiality. Each interviewee's recorded data was placed in a separate digital file. Each digital file was labeled with the assigned interview code to ensure the confidentiality of the participants. After labeling the recordings, the audio files were

saved on a compact disc. To protect the rights of the participants, all data, including the compact disc, will remain in locked fire-rated safe for 5 years.

Data Collection Instruments

The researcher was the primary data collection instrument in this study. In qualitative research, the researcher is the primary data collection instrument because the researcher sees, hears, and interprets the data (Anyan, 2013). Data collection instruments are necessary for the data collection and analysis portion of a research project (Lewis, 2015). The instrumentation for a case study can include observations, interviews, documents, and audiovisual material. Interviews, observations, and documents are appropriate for case studies (Lewis, 2015).

Four audio-recorded, semistructured interviews were conducted using an interview protocol to encourage open discussion (see Appendix F). The information contained in the interview protocol was used as a guide to conduct compelling interviews by aligning the questions with the primary research question. Bias may appear throughout the interview if the interviewees form personal assumptions.

Data sources included interviews and publicly available documents from the international card processing organization. Documents from the card-processing organization included policies, procedures, and documented proprietary card processing information. Larkin and Burgess (2013) stated that organizational documents might include the public and internal documentation. Both proprietary and publicly available documentation were used. The documentation included account agreements, card fraud

agreements, and proprietary fraud detection documentation. Bias was avoided by listening to the participants and remained open-minded to the participants' answers (Hansman, 2015).

Member checking sessions were essential for clarity and understanding of the participants' answers and understanding data presented within the organizational documentation. Validity and reliability in case studies have different methods during the research process (Morse, 2015). Validity confirmation involves transcript review (Morse, 2015). Member checking allows the researcher to document the participants' answers during data collection (Greene & Stavins, 2017).

Member checking was used to clarify and modify participants' responses to ensure the responses are correct. The member checking process allows the interviewees the opportunity to edit their responses to ensure accuracy (Fusch & Ness, 2015). The interviewees had 24 to 48 hours to review their answers and make any corrections during the member checking process. Public and internal documentation was used to validate responses to the interview questions and ensure an understanding of the participants' thoughts.

Semistructured interview questions and analysis of payment-card fraud documents serve as the data collection instruments. Different methods of data collection were used before deciding on the most appropriate information collection system for the study. Turley, Monro, and King (2016) encouraged the use of written accounts as

convenient for the narration of an event. The written accounts were transcribed interviews and field notes.

Turley et al. (2016) affirmed that semistructured interviews provide an elaborate account of events because of flexibility. Turley et al. confirmed that most researchers use individual interviews as a data collection instrument. The responses to the interview questions provided insight into the perceptions of data-security specialists to help determine the appropriate strategies for eliminating payment-card fraud.

Data Collection Technique

In this qualitative single case study research, the researcher was the primary data collection instrument. According to Patton (2015) and Yin (2014), the researchers are the primary data collection instrument in qualitative studies. Four participants from an international card processing organization located in the southeastern United States agreed to be interviewed. Case study researchers use multiple methods to collect data. The data include conversational semistructured interviews coxed by the interview guide (see Appendix G), to determine the barriers faced by the organization concerning data breach and identity theft (van Zyl, Bam, & Steenkamp, 2016).

Semistructured interviews with 11 open-ended questions were conducted. Internal documentation provided by the vice president of the card processing organization was collected. Methodical triangulation was used to enhance identified outcomes. Venkatesh et al. (2013) posited interviews are the preferred method for data collection in qualitative research. The interview guide allowed specific topics to be covered and let the

interviewer delve more in-depth into responses to gain additional knowledge (van Zyl et al., 2016). The literature review and relevant publicly available documents allowed the researcher a broader opinion and constraint barrier to addressing strategies for reducing/eliminating payment-card fraud.

The use of open-ended interview questions enabled the participants to answer freely and descriptively. Interviews were conducted away from the participants' workplace to allow for comfort while responding to interview questions. Williamson et al. (2015) suggested that the interviewees are more likely to provide descriptive detail in a comfortable setting.

Oltmann (2016) confirmed that interviews conducted in comfortable settings provide the opportunity and freedom to describe their experiences. The disadvantage of face-to-face interviews included the difficulty in setting up convenient meeting times and locations (Oltmann, 2016). An additional disadvantage was the time to collect data, cost factors, and distractions (Topkaya, 2015; Vogl, 2013). Because the interviews were open-ended, no pilot study was necessary.

The disadvantages to semistructured interviews involve the interviewee having time for the interview, and the interviewer attempting to adjust schedules to meet with the interviewee (Rahman, 2015). The differences in managerial levels and educational levels are a disadvantage that can be overcome through the researchers adjusting attitude and watching for visible clues to comfort (Irvine, Drew, & Sainsbury, 2013; Shapka, Domene, Khan, & Yang, 2016). Each interview was audio-recorded. After completing

data collection, member checking was conducted through the telephone or electronic mail, depending on the availability of the participant. Member checking assists researchers by ensuring the information captured was accurate and accurately reflects what the interviewees intended to put forward (Houghton et al., 2013; Marshall & Rossman, 2016; Morse, 2015).

The participants had the opportunity to verify their responses for accuracy, provide additional information for clarity, and provide any additional details during the member checking process. Participant information verification allows for accuracy during the member checking process (Houghton et al., 2013). The member checking process increases reliability by giving participants one additional opportunity to provide additional information or correct misconstrued information (Harvey, 2015). Reilly (2013) stated that participants might challenge information interpretation during member checking.

Data Organization Technique

Data organization allows the researcher to track references (i.e., organizational documents, peer-reviewed journal articles, books, dissertations, and conference papers). Word Add-in was used for APA format for citations and bibliographies. To ensure the Walden University requirement that 85% of the resources are peer-reviewed and within 5 years of the anticipated graduation date, an Excel spreadsheet was used that contained authors' names, article names, dates, and publication information. Microsoft Note was also used to store Adobe Reader files and notations for the study.

Xu and Storr (2013) wrote that data organization helps the researcher to remain focused on the task at hand. The identification of themes for analysis and interpretation was essential to data analysis and interpretation (Anyan, 2013). The use of methodical triangulation assisted in determining patterns or themes, prevent bias and increase reliability and validity from the use of multiple data sources.

Sanjari, Bahramnezhad, Khoshnava Foman, Shogi, and Ali Cheraghi (2014) and L. Turner (2010) recommended researchers protect their data using password protection on flash drives, computer hard drives, and cloud storage. Sanjari et al. recommended that researchers protect the identities of participants through coding of individuals, places, and organizations. L. Turner indicated information should be stored on a computer hard disk, backed up on an external drive, and stored in a fireproof safe deposit box for 5 years. Several Universal Serial Bus (USB) drives were used to compliment password-protected cloud storage on storing the information for 5 years. The purpose of the stored information is the assumption of confidential and complex passwords to prevent intrusion and discovery by unauthorized persons. Internet obtained documents were not used for data triangulation. All data for the project were stored in a separate folder. Additionally, data retention and storage met the university's requirement for 5 years from the date of anticipated graduation.

Data Analysis

De Massis and Kotlar (2014) discussed three general methods for analyzing data: (a) explanation building and within-case analysis, (b) cross-case analysis, and (c) pattern

matching. Because this was a single case study, I used within-case analysis and pattern matching. As noted by De Massis and Kotlar, in a single case study, the researcher must converge the data from various sources to understand the entire subject under study.

The researcher should identify and highlight different interpretations among case study interviewees (De Massis & Kotlar, 2014). Comparison is the primary tool in qualitative analysis researchers used to identify constructs, group the constructs into main ideas or themes, and discover contrary evidence, and so on. The primary objective of qualitative analysis is to identify conceptual similarities and differences and to discover types, classes, sequences, processes, patterns, or wholes (De Massis & Kotlar, 2014). The process of data analysis included reviewing all the collected information and organizing to generate themes. After completing the interviews, the data were transcribed into Microsoft Word. Member checking was performed by e-mailing each participant a copy of the interview transcript to ensure data accuracy. After member checking, the development of the data included categorizing key components, correlating themes, defining topics, and maintaining the participants' intent (Fusch & Ness, 2015; Hashimov, 2015).

Triangulation is the use of multiple sources or methods in a qualitative case study (Patton, 2015; Yin, 2009, 2014). Methodical triangulation was used to analyze the data obtained from interviews, internal, and external documents. The information was organized and analyzed to allow for preliminary exploration and subsequent in-depth inquiry by triangulating the interview data with the documentation supplied by the data-

security specialists. The data analysis technique involved the use of the NVivo 10 software (Robins & Eisen, 2017). The information reduction assisted with identifying relevant information about the subject matter of designing new payment-card fraud elimination strategies.

Emerging themes were observed based on both interviews and document data. Using NVivo 10 software ensured consistency and uniformity of coding (Foster, Curtis, Mitchell, Van, & Young, 2016; Houghton et al., 2017). I coded data based on conceptual similarities and differences in the interview transcripts and the documentation. I then explored the coded data searching for recurring patterns. The results of the study provided information to card processors on how to reduce payment-card fraud opportunities.

Reliability and Validity

Iwata, DeLeon, and Roscoe (2013) stated that qualitative researchers focus on credibility, transferability, dependability, and confirmability to determine the truthfulness of the relayed information by the participants. Qualitative reliability and validity help substantiate the validity of the findings, conclusions, and recommendations (Iwata et al., 2013). Following Iwata et al. template, documented data collection procedures, member checking, and methodological triangulation were used as part of the process for assuring this study's reliability and validity.

Reliability

Qualitative researchers enhance the reliability of their research by ensuring the consistency of the results rather than that of the instrument used to collect data, as in quantitative analysis (Iwata et al., 2013). *Dependability* is the achievement of the same results if the study is repeated (Morse, 2015). Rennie (2012) affirmed dependability as the ability to repeat the study with consistent findings.

Fusch and Ness (2015) and Noble and Smith (2015) noted qualitative that researchers use methodical triangulation to ensure the reliability of the study data. An interview protocol was followed to maintain consistency by asking each participant the same questions. To enhance the dependability of this study, Behrendt, Matz, and Goritz (2017) posited the importance of considering the participants' actions and responses as credible and truthful. During the interview process, the established interview protocol was followed. Methodical triangulation was used to ensure the dependability and reliability of the data used in the study. Noble and Smith identified the necessity to record all data and information gathered during the study in an accurate and accessible manner.

Validity

In qualitative research, researchers use credibility, transferability, and confirmability as the criteria for trustworthiness (Chowdhury, 2015). Nelson (2016) posited that case study researchers reach validity when the findings become confirmable

and credible. C. Marshall and Rossman (2016) noted that researchers integrate rich and detailed descriptions of themes as a strategy to increase validity in qualitative research.

Credibility. Preconceptions and researcher bias can negatively affect the validity and reliability of qualitative research; to mitigate personal bias, qualitative researchers use bracketing techniques to identify and address these preconceptions (McCarthy, 2016). Gold (2014) stated that credibility might require using member checking. Credibility was ensured by validating and expounding on interviewees' responses during the member checking process. Triangulation of the documents, interviews, and literature review may ensure additional credibility (Gold, 2014). Member checking and triangulation may aid in checking for bias, provide more information, and include other perspectives than the researchers adding credibility to the study (McCarthy, 2016; Nelson, 2016).

Transferability. Transferability, as discussed by Amankwaa (2016), shows the study findings have context for additional studies through thick descriptions. Since strategies for payment-card fraud elimination by an international payment-card processing organization located in Atlanta, Georgia, were explored, the boundaries of the study may limit the transferability of the study. Thick descriptions of the data analysis process, participants, and research context were provided to improve transferability.

Data saturation. To support the validity of the study, interviewing participants continued until data saturation was achieved. Data saturation occurred when the participants, the ones with the most knowledge, provided no new insights to the

investigative topic (O'Reilly & Parker, 2013). Interviews were reviewed in sequence and stopped when the final interview revealed no additional information.

Data saturation occurred when no added information was imparted as posited by Bagnasco, Ghirotto, and Sasso (2014) and B. Marshall et al. (2013) and O'Reilly and Parker (2013). Data saturation relates to the depth of the sample and the ability to find repetition in the information through interviewing most of the employees of a small business (Bagnasco et al., 2014; O'Reilly & Parker, 2013). In an exploratory case study design, data saturation occurs when the participants, the ones with the most knowledge, provide no new insights to the investigative topic (O'Reilly & Parker, 2013).

Transition and Summary

Section 2 covered the methodologies and strategies to investigate the phenomena of payment-card fraud and the current (2014/2015) strategies for detecting and reducing payment-card fraud. The researcher, as described by Lakshmi and Mohideen (2013), has the responsibility for accuracy and validity in their research. The interview questions follow the primary research question: *what strategies can the payment-card acceptors implement to reduce and eliminate fraud and identity theft?* The qualitative case study includes interviews and publicly available documents related to the business' data breach and fraud detection systems to gain further understanding of current 2017/2018 strategies.

Section 2 contains the methodologies and strategies to approach this study on payment-card fraud to enable the development of new fraud detection strategies. In Section 2, elaboration of the model of the study, which included a collection of data,

organization, and analysis. Also contained in this section is the data collection instrument, reliability, and validity of the data collection instrument, data organization techniques, and evaluation of data. The purpose of determining the appropriate measure to eliminate payment-card fraud continues in section 3 with the overview, provision of the results, application to professional studies, and effect on social settings. Section 3 contains the findings, conclusions, and recommendations.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative single case study was to explore strategies international card processing organizations use to minimize payment-card fraud. The results from the study revealed strategies payment card processing organizational leaders used to identify and reduce or eliminate fraudulent card transactions. The targeted population was one organization's vice president and three data security analysts at an international card processing organization in Georgia.

The organization vice president signed the letter of cooperation after receiving Walden University Internal Review Board approval to conduct the study. Data from the semistructured interviews and organizational documents were analyzed using methodological triangulation. Member checking was used to ensure the accuracy of data interpretation. Data analysis included coding techniques and member checking.

Presentation of the Findings

The overall research question for this study was what strategies do international card processing managers use to minimize payment-card fraud? The information from this study derived from interviews and public and private company documents about data security and card fraud detection. Data saturation occurred after interviewing four participants. After collecting data from four semistructured interviews, data saturation was achieved when the last participant interviewed provided no new information. Member checking validated the conclusion of data saturation. Information from the

company and public documentation and interviews were triangulated to gain a fuller understanding of the strategies card processors use to reduce and eliminate card fraud.

Cressy's fraud theory, developed in 1954, was the foundation for this study. Fraud theory was used to explore the strategies card processors could use to reduce payment-card fraud. Managers use the following key concepts (Chafjiri & Mahmoudabadi, 2018) to determine fraudulent purchases: (a) fraud risk assessment, (b) rationalization of the act, and (c) the person's motivation to commit fraud. All the participants stated in their interviews that risk assessment was essential to determining and eliminating card fraud.

Artificial intelligence, customer education, and enhanced security is essential, as confirmed by Chafjiri and Mahmoudabadi (2018) and Pigni, Bartosiak, Piccoli, and Ives (2018). Managers could use the results of this study to develop, enhance, or implement strategies to enhance data security and decrease payment card fraud. Four themes emerged from the data (a) artificial intelligence, (b) cardholder and acceptor education, (c) enhanced security strategies, and (d) PCI-DSS rules and regulations were identified from the results of this study and the conceptual framework of fraud theory.

Emergent Theme 1: Artificial Intelligence

The first theme that emerged from the data analysis was the need for the use of artificial intelligence. The four data security professionals stated AI had reduced payment card fraud by focusing on the cardholders' purchasing habits; however, DS01,

DS02, DS03, and DS04 all stated AI still is not 100% accurate. DS01 explained how AI works using customer information and purchasing patterns:

AI reduced card fraud by tracking customer usage and flagging unusual transactions or transaction times. The flag notifies the fraud department to contact the cardholder to determine if the transactions are valid. The success rate has been less than 100% due to false positives. False positives are defined as transactions that are flagged as fraud; however, the cardholder made the purchase and confirmed with the processor and holder.

DS02 further explained, “AI accuracy is less than perfect because the software being used was created by humans. The flaw in the system is the fact AI does not have the mind of a human”.

DS04 stated, “AI gives false declines to cardholders because of simultaneous purchases at the same location or at a different location.” When asked to explain the comment about simultaneous transactions for a more precise understanding and how this thought applied to accuracy, DS04 stated,

The cardholder presents his or her card at a local retailer for purchase. Someone has hacked their card information and makes a transaction on the web (card not present) at approximately the same time. AI is not smart enough to realize that the card-not-present transaction is fraudulent. The only way that the cardholder will know of the transaction has occurred is a decline or a phone call from the issuer asking about the transactions.

The accuracy issue arises because of false declines (Mohammed, Wong, Shiratuddin, & Wang, 2018). AI may cause a credit card decline by processing the transaction incorrectly (DS03). Companies use AI programs to predict fraud transactions (Mohammed et al., 2018). The programs struggle with massive amounts of concurrent transaction processing. The programmers and analysts continue to review and test advanced neural networks, also known as deep learning processes, involving the number of fraud transactions flagged versus the number of approved transactions (Mohammed et al., 2018). The payment processor uses proprietary products to detect fraud and currently is testing deep learning processes, according to DS01.

Theme 1, artificial intelligence (AI), ties in with previously published information on artificial intelligence. Mohammed et al. (2018) claimed AI continues to reduce fraud transactions, and accuracy continues to improve with the deep learning processes. Mohammed et al. confirmed AI and card fraud detection processes need enhancements to continue trapping fraud transactions without identifying false positives. Based on the systematic analysis of internal organizational documents and spreadsheets on card fraud, additional development of AI is an effective strategy to reduce card fraud.

Cressy's fraud theory, developed in 1954, was the foundation for this study. Managers use the following key concepts to determine fraudulent purchases: fraud risk assessment, rationalization of the act, and the person's motivation to commit fraud. All the participants stated in their interviews that risk assessment was essential to determining and eliminating card fraud. Cressey (1950, 1954) and Fleming et al. (2016)

explained the fraud triangle as (a) opportunity, (b) rationalization, and (c) financial pressure. Identifying fraud risk and eliminating opportunity using artificial intelligence is a significant component of assurance services.

Assessment is a crucial factor in eliminating or reducing card fraud opportunities. Transaction processors must have a clear understanding of what transactions are fraudulent. If transactions are not managed properly, the number of false declines and fraudulent transactions will increase. AI and deep learning processes continue the need for human interaction to reduce opportunities for card fraud. Additionally, based on internal documentation, spreadsheets, and interview analysis, human interaction reduces the rationalization and reasons for a person to commit card fraud.

Emergent Theme 2: Cardholder and Acceptor Education

The second theme that emerged from the data analysis was the need for cardholder and acceptor education referencing card security and usage. Payment cards are becoming a widely accepted method of payment, and security is a significant concern for both the cardholder and the acceptor. Payment cards can be exploited physically or virtually. The virtual exploitation takes place with card not present purchases of goods and services.

The physical exploitation takes place when the person presents the card to pay for goods or services. The potential for physical exploitation lies with the card reader that may or may not have been tampered with, the server at the restaurant, or even cashier at a local retail establishment. The four participants stated that cardholder and acceptor

education is key to reducing and eliminating card fraud. DS01 and DS02 provided in-depth discussions about how cardholders and acceptors need to focus on security education.

DS01 stated,

Cardholders need to be more aware of surroundings when using their cards for purchases. Should the cardholder find they are in an unfamiliar area or see people hanging around that makes the cardholder uncomfortable about using their card, do not use the card. If the automated teller machine or point of sale equipment looks like it has been tampered with, do not use the machine, as a card skimmer may have been installed. Card skimmers read the stripes on the card and obtain the cardholder information.

DS02 further stated,

Notify the authorities such as police, bank, store manager, and even businesses like MasterCard and Visa that the machine has been tampered with. You as the cardholder may not be the only one that has been victimized by the machine.

When notifying the appropriate people, be sure to provide the location, time of day of discovery, and lock your card with the issuer. One last organization to notify is the credit bureau.

When asked why victims should contact the credit bureau about card fraud, DS02 stated,

Notifying the credit bureau may slow down fraudulent accounts in the victim's name. By checking credit reports regularly, people can review their report and see what accounts are open, what attempts for new credit has been made. During the process, if the person sees something that is not correct, the person has the right to dispute the inquiry and or account.

DS01 and DS03 stated informed cardholders check their accounts, review statements, dispute charges, and regularly check their credit reports. The participants' responses confirmed Greene and Stavins' (2017) conclusions that cardholders and that acceptors need to learn the best strategies to protect card information and data. Greene and Stavins and Ghazali et al. (2019) noted acceptors and processors should build trust that their transaction processing system is secure, and their companies use third-party verification systems.

Ghazali et al. (2019) further stated card transaction processors should generate a random six-digit number for the consumer to enter at the payment terminal and use multiple encryption levels based on secure socket layer (SSL) during the transaction processing. DS03 suggested strongly cardholders pay closer attention to payment card equipment at the checkout; if the equipment looks damaged or tampered with, do not use the machine. Instead, DS03 recommended the cardholder use cash or other payment instruments (e.g., checks or gift cards). DS02 explained,

Fraudulent charges may be detected or blocked when you travel outside your normal consumer area. Example: International travel – debit/credit card transactions decline, and you are stuck at the airport or port of call without a way to make purchases. The cardholder has the option to contact the issuer to let the issuer know they are out of the country. In-country, travel may also cause a card to decline if the cardholder does not normally travel either internationally or locally.

Detection occurs when cardholders travel to areas outside of their consumer area or make purchases that are out of the ordinary.

DS01 discussed educating consumers to use pre-paid cards or PayPal as means to make online purchases and travel. DS01 recommended the use of PayPal because the user can set aside a certain amount for their online purchases, place the funds in the PayPal account, and transfer the funds.

The safety, as described by DS01 and DS02, is that PayPal only has what the user puts in the account. If someone gets the password to the account, the user is not ruined financially. Deposit Agreement and Disclosures documentation describe the consumers' liability as \$0 from unauthorized transactions, so the cardholder will not be held responsible for fraudulent purchases. The organization's deposit agreement and disclosures documentation indicate the processor provides the customer with immediate notification of essential activities such as a low balance or large transactions, which may be fraudulent.

Additional education steps discussed by DS01 and DS03 addressed replacing card reader equipment. Current equipment reads both chip and magnetic stripe cards. The magnetic stripe reader enabled thieves to clone cards easily (Banker, D'Amato, & Sheridan, 2008). Banker et al. (2008) concluded replacing magnetic stripe cards with chip and pin cards and replace all card processing machines with chip and pin enabled card readers. Banker et al. stated that card acceptors would be likely to change their equipment if there were incentives to upgrade or purchase new card readers. The replacement of the card readers would reduce fraud opportunities (Banker et al., 2008) by using the newest technologies.

Education is an additional key to reducing or eliminating card fraud opportunity as described by Cressey (1954) and Fleming et al. (2016). Fraud theory states that people commit fraud because of opportunities, rationalization, and peer pressure. Theme 2 extends the knowledge of payment card security for the cardholder and acceptor through education and information provided by card issuers.

Card acceptors and processors should focus on upgrading card reader hardware. If the equipment is not updated and, the servers are not kept up to date with antivirus tools, malware detection, and adware detection opportunities for fraud will continue to exist. DS02 stated their company's processor's servers have the latest in fraud detection methods installed (a) enhanced firewalls, (b) the latest malware, (c) spyware, and (d) virus updates are applied to their network. The results of the current study indicate that upgrades are necessary to reduce or eliminate payment card fraud. Internal

organizational documents were not available to support the above; however, new literature has been written stating that educating cardholders and processors reduce card exploitation.

Emergent Theme 3: Enhanced Wireless Security Strategies

More robust protection strategies were the third theme to evolve from in-depth analysis of the participants' interviews, and reviews of public and private documentation on network security. All the data security analysts responded that more reliable protection strategies are needed to combat card fraud. While more robust protection strategies include enhanced artificial intelligence (AI) and education, DS01 and DS03 commented that small business card transactions on unsecured wireless home-style routers leave the cardholder open to fraud and identity theft opportunities.

Company documentation provided information about wireless security and the strengths and weaknesses of home-style routers. Wireless security may be turned on; however, the security of the small business' wireless router may not be as secure as the business owner may think, according to DS01. The home-style router typically uses Wired Equivalent Privacy (WEP). Sari and Karay (2015) posited WEP protocols are a weak security protocol lacking management and authentication features. DS02, DS03, and DS04 all noted wireless connections are not secure and are the easiest way for someone to obtain cardholder information.

WEP security uses static keys for both authentication and encryption. Once the key is decrypted, the key can be used to decrypt all the packets (Akomea-Agyin &

Asante, 2019) in data transmissions. Attackers can use the process to obtain user information and passwords. The second reason WEP is not the right choice for security is that the protocol does not support mutual authentication. Additionally, WEP uses 24-bit encryption, which opens the security protocol to reuse attacks. Finally, WEP uses a linear process for checksum integrity, which enables attackers to inject messages to return information to the wrong system. The WEP encryption process is entirely insecure, no matter how secure the encryption keys may be. The opportunity that the WEP protocol presents fraudsters to spoof web sites and obtain consumer information.

Online consumers continue to encounter vulnerability when making purchases. The website may look legitimate, yet the site could have been spoofed. Rivera (2018) described spoofed websites as websites that look legitimate; however, the site has been cloned or spoofed to obtain cardholder information. DS04 stated, “Consumers may input their payment information and receive confirmation of the funds' transfer, yet what the consumer doesn't realize is the information they input has gone to the dark web.”

The dark web, according to Rivera (2018), poses vulnerability threats to businesses. The vulnerabilities are hard to close because of the different security protocols required by each country (Rivera, 2018). All participants stated the dark web would continue to be a primary concern as criminals continue to exploit security vulnerabilities. Technological advancements in web crawlers, monitoring, and intelligence gathering methodologies are currently thriving in removing dark web sites

from the Internet; however, significant gaps still exist in the monitoring of dark web sites (Paul, 2018). New security strategies are needed to combat fraud on the dark web.

The dark web has become the primary concern as acceptors and processors address security vulnerabilities caused by spyware, adware, malware, and virus detection (Rivera, 2018). The opportunity for card fraud remains in the card-not-present (CNP) transaction area. Cardholders need to be aware of websites and phone shopping as the sites may look legitimate but are set up to defraud the cardholder.

In discussing fraud theory, Omar et al. (2016) noted that the person committing the fraudulent act is not likely to be caught. The completion of fraudulent purchases occurs before the victim tries to use their account to make a purchase. Payment-card fraudsters realize the act of committing fraud requires both ability and the perception that he or she may not be caught (Craig & Piquero, 2016; Omar et al., 2016). DS03 indicated that small business owners should use more robust security system settings for their networks and credit card processing machines.

Enhanced security strategies, cardholder and transaction processor education, and artificial intelligence play critical roles in reducing or eliminating card fraud. Improved strategies in card-not-present transactions should reduce credit card fraud. Business owners who process transactions need to understand the vulnerabilities created by the dark web and how to combat them. Business owners must ensure their wireless technology has secure security protocols to protect consumers.

Emergent Theme 4: PCI-DSS Rules and Regulations

Emergent Theme 4 focuses on PCI-DSS rules and regulations. The purpose of the Payment Card Industry Data Security Standard (PCI-DSS) is to outline technical and operational requirements to protect data (PCI Security Council, 2018). Business leaders whose businesses store, process, or transmit data should be aware of and follow these regulations. Each of the participants conveyed the necessity for more definite PCI-DSS rules and regulations for card issuers, acceptors, and processors. PCI-DSS regulations recommend that card-accepting merchants use some form of security to protect customer data.

DS02 and DS04 stated that small and medium-sized business owners need to have training in PCI-DSS rules and regulations from PCI-DSS experts in storing customer data to reduce identity theft or card fraud opportunities. The training should cover secure data backups and checking the ID of the cardholder to reduce fraud opportunities. PCI-DSS rules and regulations state backups must be stored off-site. The checking of the ID of the card user is a strong recommendation from the experts at PCI-DSS to reduce identity theft opportunities.

DS03 stated,

The easiest place for a data breach is the gas pump. Consumers place their cards in the reader and enter their personal identification number. The gas pump card reader may have been tampered with and a card skimmer placed in the card slot on the pump. The consumer is unaware of the skimmer.

PCI-DSS regulations require that the card acceptors clear the information after the customer completes his or her transaction from the card reader. Not all card acceptors clear card information after a transaction (Piazza, Fernandes, Anderson, & Olmstead, 2016). By not clearing the data from the processing computer system, the retailer is in danger of exposing the customers' data to theft.

The theft of customer data costs business millions every year (Graves, Acquisti, & Christin, 2018). One data breach incident may take several years for a business to recover its reputation and financial losses (Graves et al., 2018). DS02 stated that business leaders must decide what the cost of doing business, as a PCI-DSS compliant organization, is compared to the cost of the loss due to card theft and data breaches. The cost of doing business factors slowly into what a business can consider as an acceptable loss due to fraud (Graves et al., 2018).

DS04 stated that fraud losses could be minimized through other means. The means recommended by DS04 involved the usage of hologram cards in reducing card fraud and data theft opportunities and meets the PCI-DSS data storage requirements, as holograms are harder to detect. The newest technologies use cloud-based transaction processing. The cloud-based transaction uses a card hologram that disappears after the transaction completes. Also, cloud-based processing prevents attacks from RAM scrubber malware (Saravanan & Suresh Babu, 2017).

PCI-DSS regulations describe how card issuers and payment processors must not store Personal Identification Numbers (PIN) or the card validation code. PCI-DSS

requires all card acceptors and processors to use a truncation of the card number and encrypted drive storage and back-ups. DS04 stated hologram cards store limited data such as the last four numbers of the payment card. Hologram card readers only show a masked version of the payment card and a tokenized representation of the card holder's information (Piazza et al., 2016). Piazza et al. (2016) stated that the tokenized version of the cardholder's information is harder for malware to attack and strip customer information.

The card validation code is used for card-not-present transactions. The 3- or 4-digit security code imprinted on the card is intended for card-not-present purchases to ensure the card is in the customer's possession (Carneiro et al., 2017). PCI-DSS regulations focus on card-present and card-not-present transactions. Implementation of PCI-DSS regulations has a large dollar amount for the upfront cost. According to DS01, "Implementation of PCI-DSS regulations involves network appliances such as firewalls, routers and switches, and software costs. The software included malware and virus detection software. The software should be updated regularly".

Most small business owners, according to DS01 and DS02, are not in a financial position to implement a full PCI-DSS implementation. Fleming et al. (2016) discussed how fraudsters justify committing fraud through (a) a moral justification, (b) feeling the organization owes them something, and (c) rationalization. Fraudsters rationalize the theft by claiming the business owes them for poor working conditions (Omar et al.,

2016). The opportunity that PCI-DSS rules and regulations attempt to close is the wireless connections.

Small to medium-sized businesses are not in financial positions to do a full PCI-DSS investigation and installation. The regulations are only recommendations. Yulianto, Lim, and Soewito (2016) posited that the security program should be comprehensive and cover all areas of security. The PCI-DSS rules and regulations are only guidelines.

Usage is voluntary and costly for most smaller businesses.

Table 1

Total of Direct Quotes and Documents for Themes 1, 2, 3, and 4

Theme	DS01	DS02	DS03	DS04	Documents
Theme 1	6	5	5	6	6
Theme 2	5	5	7	7	5
Theme 3	5	7	8	5	9
Theme 4	6	7	5	5	5
Total	22	24	25	23	25

Applications to Professional Practice

Innovative approaches are needed to combat card fraud. Data collected from interviews indicated that small businesses' current fraud detection strategies need further enhancements to reduce or eliminate card fraud. The outcome results are essential for this study. The participants in the current study focused on enhancing artificial intelligence, educating cardholders, and processors to detect fraud situations, enhancing wireless security, and increasing adherence to PCI-DSS rules and regulations.

The literature supported the four themes found in this study and Cressey's (1954) fraud theory. Using the tenets of fraud theory to enhance fraud detection methods could decrease identity theft and increase card fraud detection (Sadgali, Sael, & Benabbou, 2019). The correlation of fraud theory to card transactions relies on fixed processes and rules to determine fraud that is outdated and needs enhancements (Robinson & Aria, 2018).

Card processing organizations that apply fraud theory could solve payment card fraud quickly and efficiently. According to Manworren et al. (2016), the number of payment card fraud and identity thefts continues to rise because of the number of interconnected devices. The case for card fraud detection (cybersecurity) is growing more durable; the card processing management team that adapts cybersecurity will be more sustainable and strategically placed than card processing organizations that do not (Manworren et al., 2016).

All four participants emphasized the importance of artificial intelligence and the need for enhancements. Mohammed et al. (2018) stated that AI and card fraud detection processes need enhancements to continue identifying fraud transactions without identifying false positives. The theme of the cardholder and card acceptor education was the second theme discovered during interviews and analysis. Education was important for three of the participants, as they realized that everyone does not know what the indicators of card fraud involve. Greene and Stavins (2017) concluded that cardholders and acceptors need to learn the best strategies to protect cards and information and data.

Two of the participants discussed the importance of enhanced wireless security and the dark web. Rivera (2018) and Sari and Karay (2015) concluded that home-style wireless routers using WEP security enables fraudsters to obtain data and make it available on the dark web. Three of the participants commented on the need for PCI-DSS rules and regulations to be enhanced. The rules and regulations define the rules for card acceptors; however, not all card acceptors and processors can afford to have a full PCI-DSS evaluation and implementation (Yulianto et al., 2016).

Implications for Social Change

When security analysts and managers who work for payment card processing organizations implement strategies to reduce or eliminate payment-card fraud, they protect their organizations, consumers, and the local and national economy. The reduction of card fraud and data breaches includes the potential for new jobs, lower consumer prices, reduced business insurance costs, and enhanced revenue for local businesses, contributing to the local economy. The continued usage of payment cards may help sustain economic growth, improve vendor relations, and may contribute to the promotion of other social activities (Lee, 2018).

Increased credit card fraud will reduce overall profits for banking, processors, and card acceptors (Mahmoudi & Duman, 2015). Data security managers who implement effective strategies may reduce payment card fraud by implementing new fraud detection strategies. The outcome of this study may enhance social change by increasing consumer confidence and promote economic growth. The adoption of the strategies that data

analyst managers use may affect social change by increasing fraud detection, decreasing data breaches, increasing consumer satisfaction, and preventing identity theft. The consequences of identity theft can follow individuals for a lifetime by compromising their social security numbers, ability to get future credit, or incurring additional debt.

Consumers are more likely to continue to use their cards for online and brick and mortar purchases when they see decreased chances for card fraud. Decreasing criminal activity reduces costs for all businesses, and thus both the business and the consumer benefit by higher profits and lower costs. Particularly following economic times of stress like the coronavirus pandemic of 2020, protecting businesses and the consumer is of tantamount importance.

Recommendations for Action

In the United States, payment card fraud and data breaches affect 3 million people annually. According to Tatham (2018), payment card fraud accounts for \$905 million of liability in 2017. For payment card fraud detection, four recommendations were uncovered (a) continue to enhance and implement artificial intelligence, (b) educate the cardholder and acceptor in what to look for when using/accepting payment cards, (c) enhance security for wireless networks at small to medium-size businesses, and (d) follow PCI-DSS rules and regulations for storing personal data. The four recommendations should benefit card processing organization managers who are struggling to reduce or eliminate card fraud.

The findings of this study indicated the need for increased payment card security. All the participants indicated that a sharper focus on security would have a positive effect on reducing or eliminating card fraud. A recommendation focusing on enhancing the programming for artificial intelligence, educating cardholders and acceptors, using alternate methods for transmitting data such as a virtual private network (VPN), and following the PCI-DSS rules for clearing out card readers and storing customer information is offered.

Secondly, for card processing organizations to remain successful, managers should focus on keeping the security of their networks up to date with the latest virus signature, operating system updates, and the latest malware/adware updates. The results of this study revealed that card processing organization managers who improve transaction security continue to stay in operation. Results of this study will be offered for dissemination through publications in the ProQuest Dissertation and Theses Database, distribution to participants, and presentations at professional conferences and business-related forums when applicable.

Recommendations for Further Research

The study was delimited to the southeast region of the United States and a single payment card transaction organization. The primary limitations of this study resulted from (a) use of only one theory of fraud; (b) geographical location; (c) and, focus on one international card transaction processing organization. For further study, I recommend

exploring other card transaction processing organizations in other regions of the United States.

Other researchers may use different theories, methodologies, and designs to collect information from other card transaction processors to explore reliable strategies for card fraud reduction and elimination. Future researchers should study the fraud theory to explore the effect of technological advances in card transaction fraud processing. Quantitative analysis may be useful in determining which strategies are most successful in reducing or eliminating fraud by surveying many credit card processors to determine which methods they use and how successful they are in reducing fraud over time. Future researchers should consider exploring the impact of these initiatives on consumers' willingness to use credit cards after a data breach has occurred.

Reflections

As I reflect on my journey, I encountered multiple roadblocks and achievements. Early on, I encountered homelessness. The feeling of not knowing where I would sleep, eat, or even if I would survive until the next day was resolved by someone who became a good friend. My study is dedicated to this person. I lost my friend, confidante, and mentor in 2015. Also, during my journey, I gained an extended family. My extended family has helped to keep my sanity and keep me focused on my studies. The journey has been long and rewarding.

My doctoral journey prepared me for the academic research tools to become an ambassador for social change. The strategies for payment card fraud reduction were

informative and yet challenging. The challenges faced were getting participants and organizations to even read e-mails or return calls. My search ended when I met the wife of the vice president of my participant organization in a doctoral program. He was in hopes that by his assisting with my study, his wife would get the same assistance when she was at the point of data collection.

Additional challenges came with work, life balance, and time management. The journey taught me a lot about myself and about how I could overcome those challenges in life that slam doors. This journey has prepared me to move forward and look at new business opportunities and continue growth, both personally and professionally.

Conclusion

The purpose of this qualitative single case study was to explore strategies that payment card processors use to reduce or eliminate card fraud. I conducted semistructured interviews with four data analysts with 10 or more years' experience working with payment card fraud. The participants all reside in the southeast United States and work for an international card processing organization.

Member checking was used to ensure data saturation and validity. Data saturation was reached when the four participants relayed similar information to answer the primary research question. The analysis of each emergent theme was linked back to the literature review, new and existing bodies of information, and the conceptual framework for the study.

In conclusion, the strategies payment card processors use to determine fraudulent transactions are artificial intelligence, more robust protection strategies, cardholder education, and PCI-DSS rules and regulations. International card processors, issuers, and acceptors need to *think creatively* and research activity on the dark web to reduce or eliminate online card fraud. Brick and mortar card acceptors need to consider the means they use to upload the customers' information to the financial institution.

Additionally, retailers need to consider how often they must perform maintenance needs on their card machines and update their inhouse computer systems. Frequent updates for malware, spyware, and antivirus signatures help to slow down data breaches and potential customer data capture. Card processors and acceptors must maintain their information according to PCI-DSS guidelines to ensure continued safe card usage. The findings of this study could contribute to positive social outcomes and help improve the reduction or elimination of payment card fraud.

References

- Abdullahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 5(4), 38-45. doi:10.6007/IJARAFMS/v5-i4/1823
- Akomea-Agyin, K., & Asante, M. (2019). Analysis of security vulnerabilities in wired equivalent privacy (WEP). *International Research Journal of Engineering and Technology*, 6(1), 529- 536. Retrieved from <http://www.irjet.net>
- Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, 23(3), 121-127. Retrieved from <http://www.tuckerpublish.com/jcd.htm>
- Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A focus on qualitative research interview. *The Qualitative Report*, 18(18), 1-9. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Azrina, M. Y., & Ling Lai, M. (2014). An integrative model in predicting corporate tax fraud. *Journal of Financial Crime*, 21, 424-432. doi:10.1108/JFC-03-2013-0012
- Applebaum, L. (2014). From whining to wondering: Reflective journaling with preservice educators. *Journal of Jewish Education*, 80, 5-23. doi:10.1080/15244113.2014.880140
- Bagnasco, A., Ghirotto, L., & Sasso, L. (2014). Theoretical sampling. *Journal of Advance Nursing*, 70, e6-e7. doi:10.1111/jan.12450

- Bai, F., & Chen, X. (2013). Analysis on the new types and countermeasures of credit card fraud in mainland China. *Journal of Financial Crime*, 20, 267-271. doi:10.1108/jfc-03-2013-0022
- Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, 51, 134-142. doi:10.1016/j.eswa.2015.12.030
- Bancroft, A., & Reid, P. S. (2016). Challenging the techno-politics of anonymity: The case of cryptomarket users. *Information, Communication & Society*, 20, 497-512. doi:10.1080/1369118X.2016.1187643
- Banker, K. J., D'Amato, J., & Sheridan, P. (2008). Credit card fraud: Awareness and prevention. *Journal of Financial Crime*, 15, 398-410. doi:10.1108/13590790810907236
- Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods*, 27, 3-21. doi:10.1177/1525822X14526838
- Behrendt, P., Matz, S., & Goritz, A. S. (2017). An integrative model of leadership behavior. *The Leadership Quarterly*, 28, 229-244. doi:10.1016/j.leaqua.2016.08.002
- Bell, E., Bryman, A., & Harley, B. (2015). *Business research methods* (5th ed). Oxford, UK: Oxford University Press.

- Benia, L. R., Hauck-Filho, N., Dillenburg, M., & Stein, L. M. (2015). The NICHD investigative interview protocol: A meta-analytic review. *Journal of Child Sexual Abuse, 24*, 259-279. doi:10.1080/10538712.2015.1006749
- Berezina, C., Cobanoglu, B., Miller, B. L., & Kwansa, F. A. (2010). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management, 24*, 991-1010. doi:10.1108/09596111211258883
- Bergman, K. M. (2015). A target to the heart of the first amendment: Government endorsement of responsible disclosure as unconstitutional. *Northwestern Journal of Technology and Intellectual Property, 13*(2), 117-151. Retrieved from <https://scholarlycommons.law.northwestern.edu/njtip/>
- Bhatia, S., Bajaj, R., & Hazari, S. (2016). Analysis of credit card fraud detection techniques. *International Journal of Science and Research, 5*(3), 1302-1307. Retrieved from <http://www.ijsr.net>
- Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditor's risk judgments. *Journal of Accounting and Public Policy, 34*, 578-596. doi:10.1016/j.jacpubpol.2015.05.006
- Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Lapedes, P. D. (2000). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. *Accounting Horizons, 14*, 441-454. doi:10.2308/acch.2000.14.4.441

- Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2018). Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Computers & Electrical Engineering*, *66*, 353-368. doi:10.1016/j.compeleceng.2017.10.012
- Chafjiri, M. B., & Mahmoudabadi, A. (2018). Developing a conceptual model for applying the principals of crisis management for risk reduction on electronic banking. *American Journal of Computer Science and Technology*, *1*, 31-38. doi:10.11648/j.ajest.20180101.15
- Cagalj, M., Perkovic, T., Bugaric, M., & Li, S. (2015). Fortune cookies and smartphones: Weakly unrelayed channels to counter relay attacks. *Pervasive and Mobile Computing*, *20*, 64-81. doi:10.1016/j.pmcj.2014.09.002
- Calderoni, F., Brunetto, D., & Piccardi, C. (2016). Communities in criminal networks: A case study. *Social Networks*, *48*, 116-125. doi:10.1016/j.socnet.2016.08.003
- Caldwell, T. (2014). Securing the point of sale. *Computer Fraud & Security*, *12*, 15-20. doi:10.1016/S1361-3723(14)70557-3
- Canadian Bankers Association. (2014). *Preventing fraud*. Toronto, Canada. Retrieved from http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/h_00122.html
- Card present. (2014). In *Black's law dictionary* (10th ed.) (B. A. Garner, editor in chief). St. Paul, MN: Thompson Reuters. Retrieved from <https://thelawdictionary.org/card-present/>

- Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining system for credit-card fraud in e-tail. *Decision Support Systems, 95*, 91-101. doi:10.1016/j.dss.2017.01.002
- Chang, C., Venkatasubramanian, K. K., West, A. G., & Lee, I. (2013). Analyzing and defending against web-based malware. *ACM Computing Surveys, 45*(4). doi:10.1145/2501654.2501663
- Chang, J.-S., & Chang, W.-H. (2014). Analysis of fraudulent behavior strategies in online auctions for detecting latent fraudsters. *Electronic Commerce Research and Applications, 13*, 79-97. doi:10.1016/j.elerap.2013.10.004
- Chowdhury, I. A. (2015). Issue of quality in qualitative research: An overview. *Innovative Issues and Approaches in Social Sciences, 8*(1), 142-162. doi:10.12959/issn.1855-0541.IIASS-2015-no1-art09
- Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences; Weaverville, 19*(1), 54-67. Retrieved from <http://www.alliedacademies.org/management-information-and-decision-sciences/>
- Clough, J. (2015). Towards a common identity? The harmonization of identity theft laws. *Journal of Financial Crime, 22*, 492-512. doi:10.1108/JFC-11-2014-0056
- Craig, J. M., & Piquero, N. L. (2016). Sensation offending: An application of sensation seeking to white-collar and conventional crimes. *Crime and Delinquency, 63*, 1363-1382. doi:10.1177/0011128716674707

- Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review*, 15, 738-743. doi:10.2307/2086606
- Cressey, D. R. (1954). Other people's money. A study in the social psychology of embezzlement. *American Sociological Review*, 19, 362-363. doi:10.2307/2087778
- Cross, C., & Kelly, M. (2016). The problem of "white noise": Examining current approaches to online fraud. *Journal of Financial Crime*, 23, 806-818. doi:10.1108/JFC-12-2015-0069
- Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, 41, 4915-4928. doi:10.1016/j.eswa.2014.02.026
- DeFeo, D. J. (2013). Toward a model of purposeful participant inclusion: Examining deselection as a participant risk. *Qualitative Research Journal*, 13, 253-264. doi:10.1108/QRJ-01-2013-0007
- De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, 5, 15-29. doi:10.1016/j.jfbs.2014.01.007
- Dilla, W. N., Harrison, A. J., Mennecke, B. E., & Janvrin, D. J. (2013). The assets are virtual, but the behavior is real: An analysis of fraud in virtual worlds and its implications for the real world. *Journal of Information Systems*, 27, 131-158. doi:10.2308/isys-50571

- Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher*, 20(5), 28-32. doi:10.7748/nr2013.05.20.5.28.e327
- Dorminey, J., Scott Fleming, A., Kranacher, M.-J., & Riley, Jr., R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27, 555-579. doi:10.2308/iace-50131
- Dorrian, J., Grant, C., & Banks, S. (2017). An industry case study of ‘stand-up’ and ‘sleepover’ night shifts in disability support: Residential support workers perspectives. *Applied Ergonomics*, 58, 110-118. doi:10.1016/j.apergo.2016.05.016
- Dudley, L., Gamble, C., Allam, A., Bell, P., Buck, D., Goodare, H., . . . Young, B. (2015). A little more conversation please? Qualitative study of researchers’ and patients’ interview accounts of training for patient and public involvement in clinical trials. *Trials*, 16, 190-190. doi:10.1186/s13063-015-0667-4
- Dusek, G. A., Yurova, Y. V., & Ruppel, C. P. (2015). Using social media and targeted snowball sampling to survey a hard-to-reach population: A case study. *International Journal of Doctoral Studies*, 10, 279-299. doi:10.28945/2296
- Ekinci, Y., Ulengin, F., Uray, N., & Ulengin, B. (2014). Analysis of customer lifetime value and marketing expenditure decisions through a Markovian-based model. *European Journal of Operational Research*, 227, 278-288. doi:10.1016/j.ejor.2014.01.014

- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Technology, 9*, 323-337. doi:10.28945/3325
- Federal Trade Commission. (1998). *Identity theft and assumption act*. Washington, D.C. Retrieved from <https://www.ftc.gov/node/119459>
- Fernandes, J. J. (2015). Get ready for PCI DSS 3.0 with real-time monitoring. *Computer Fraud & Security, (2)*, 17-18. doi:10.1016/S1361-3723(15)30009-9
- Finklea, K. (2017). Dark web. *Congressional Research Service, 7-5700*. Retrieved from https://aquadoc.typepad.com/files/crs_dark_web_10march2017.pdf
- Fleming, A. S., Hermanson, D. R., Kranacher, M. J., & Riley, Jr., R. A. (2016). Financial report fraud: Public and private companies. *Journal of Forensic Accounting Research, 1*, A27-A41. doi:10.2308/jfar-51475
- Fossi, M., Johnson, E., Turner, D., Mack, T., Blackbird, J., McKinney, D., . . . Gough, J. (2009). Executive summary: Symantec report on the underground economy. *The Journal of Financial Services Technology, 3*(1), 77-81. Retrieved from <http://www.fsprivatewealth.com.au>
- Foster, K., Curtis, K., Mitchell, R., Van, C., & Young, A. (2016). The experiences, unmet needs and outcomes of parents of severely injured children: A longitudinal mixed methods study protocol. *BMC Pediatrics, 16*, 152. doi:10.1186/s12887-016-0693-

- Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling and Development, 91*, 184-194. doi:10.1002/j.1556-6676.2013.0085.x
- Friesen, P., Kerns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont Report? *The American Journal of Bioethics, 17*(7), 15-21. doi:10.1080/15265161.2017.1329482
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Gandy, M. (2014). *Recycling and the politics of urban waste*. London, England: Earthscan.
- Ganesan, R. (2016). Stepping up security with password management control. *Network Security, (2)*, 18-19. doi:10.1016/S1353-4858(16)30019-8
- Ghazali, O., Leow, C. Y., Qaiser, S., Pattabiraman, N., Vasuthevan, S., Abdusalam, E., & Barakat, M. M. (2019). Cloud-based global online marketplaces review on trust and security. *International Journal of Interactive Mobile Technologies, 13*(4), 96-115. doi:10.3991/ijim.v13i04.10523
- Gold, S. (2014). The evolution of payment card fraud. *Computer Fraud & Security, (3)*, 12-17. doi:10.1016/s1361-3723(14)70471-3
- Graves, J. T., Acquisti, A., & Christin, N. (2018). Should credit card issuers reissue cards in response to a data breach? Uncertainty and transparency in metrics

for data security policymaking. *ACM Transactions on Internet Technology*, 18(4). doi:10.1145/3122983

Greene, C., & Stavins, J. (2017). Did the target data breach change consumer assessments of payment card security. *Journal of Payments Strategy & Systems*, 11(2). Retrieved from <https://www.henrystewartpublications.com/jpss>

Griffin, J., Abdel-Monem, T., Tomkins, A., Richardson, A., & Jorgensen, S. (2015). Understanding participant representativeness in deliberative events: A case study comparing probability and non-probability recruitment strategies. *Journal of Public Deliberations*, 11(1). Retrieved from <http://www.publicdeliberation.net/jpd/>

Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using artificial immune system. *Applied Soft Computing*, 24, 40-49. doi:10.1016/j.asoc.2014.06.042

Hansman, C. A. (2015). Training Librarians as qualitative researchers. Develop skills and knowledge. *The Reference Librarian*, 56, 274-294. doi:10.1080/02763877.2015.1057683

Hart, S. (2013). The crash of Cougar Flight 491: A case study of offshore safety and corporate social responsibility. *Journal of Business Ethics*, 113, 519-541. doi:10.1007/s10551-012-1320-8

- Hardekopf, B. (2015, January 13). The big data breaches of 2014. *Forbes*. Retrieved from <http://www.forbes.com/>
- Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, 38, 23-38. doi:10.1080/174372X.2014.914487
- Harvey, P. (2013). The road to payment card industry compliance: One company's journey. *Journal of Payments Strategy & Systems*, 7(2), 186-188. Retrieved from <https://www.henrystewartpublications.com/jpss>
- Hashimov, E. (2015). Book reviews: Qualitative data analysis: A Methods Sourcebook And The Coding Manual For Qualitative Researchers. Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña. Thousand Oaks, CA: SAGE, 2014. 381 pp. Johnny Saldaña. Thousand Oaks, CA: SAGE, 2013. 303 pp. *Technical Communicatoin Quarterly*, 24, 109-112. doi:10.1080/10572252.2015.975966
- Hoffman, K. (2013). Store opening. *SC Magazine: For IT Security Professionals (15476693)*, 24(7), 20-24. Retrieved from <https://www.scmagazine.com/>
- Holmberg, U., & Madsen, K. (2014). Rapport operationalized as a humanitarian interview in investigative interview settings. *Psychiatry, Psychology and Law*, 21, 591-610. doi:10.1080/13218719.2013.873975
- Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, 20(4), 12-17. doi:10.7748/nr2013.03.20.4.12.e326

- Houghton, C., Murphy, K., Casey, D., Meehan, B., Thomas, J., & Brooker, D. (2017). From screening to synthesis: Using NVivo to enhance transparency in qualitative evidence synthesis. *Journal of Clinical Nursing, 26*, 873-881. doi:10.1111/jocn.13443
- Huh, J. H., Verma, S., Rayala, S. S. V., & Bobba, R. B. (2017). I don't use Apple Pay because it's less secure: Perception of security and usability in mobile. *mHealth, 3*(3), 15-41. Retrieved from <http://www.thejournalofmhelath.com>
- Irvine, A., Drew, P., & Sainsbury, R. D. (2013). Am I not answering your questions properly? Clarification, adequacy and responsiveness in semistructured telephone and face-to-face interviews. *Qualitative Research, 13*, 87-106. doi:10.1177/1468794112439086
- Iwata, B. A., DeLeon, I. G., & Roscoe, E. M. (2013). Reliability and validity of the analysis screening tool. *Journal of Applied Behavior Analysis, 46*, 271-284. doi:10.1002/jaba.31
- Jacob, S. A., & Furgerson, S. P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *The Qualitative Report, 17*(42), 1-10. Retrieved from <https://nsuworks.nova.edu/tqr/>
- Jha, S., & Westland, J. C. (2013). A descriptive study of credit card fraud pattern. *Global Business Review, 14*, 373-384. doi:10.1177/0972150913494713
- Kabir, M. R., Onik, A. R., & Samad, T. (2017). A network intrusion detection framework based on Bayesian network using wrapper approach. *International Journal of*

Computer Applications, 166(4), 13-17. Retrieved from

<https://www.ijcaonline.org/>

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

Kaiser, S. B. (2013). *Fashion and cultural studies*. London, United Kingdom: Bloomsbury Publishing.

Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, 3, 191-195. Retrieved from <http://jetems.scholarlinkresearch.com>

Kerwin-Boudreau, S., & Butler-Kisber, L. (2016). Deepening understanding in qualitative inquiry. *The Qualitative Report*, 21(5), 956-971. Retrieved from <http://nsuworks.nova.edu/tqr/>

Khanna, R. (2013). Data breaches: The enemy within. *Computer Fraud & Security*, 8, 8-11. doi:10.1016/S1361-3723(13)70071-X

Kim, H., Sefcik, J. S., & Bradway, C. (2016). Characteristics of qualitative descriptive studies: A systematic review. *Research in Nursing & Health*, 40, 23-42. doi:10.1002/nur.21768

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers and Security*, 58, 39-46. doi:10.1016/j.cose.2015.12.001

- Knight, A., & Saxby, S. (2014). Identity crisis: Global challenges of identity protection in a networked world. *Computer Law & Security Review*, 30, 617-632.
doi:10.1016/j.clsr.2014.09.001
- Lakshmi, S., & Mohideen, M. A. (2013). Issues in reliability and validity. *International Journal of Management Research and Reviews*, 3, 2752-2758.
Retrieved from <http://www.ijmrr.com>
- Larkin, R., & Burgess, J. (2013). The paradox of employee retention for knowledge transfer. *Employment Relations Record*, 13, 32-43. Retrieved from <http://iera.net.au>
- Lee, Y. S. (2018). Government guaranteed small business loans and regional growth. *Journal of Business Venturing*, 33, 70-88. doi:10.1016/j.jbusvent.2017.11.001
- Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, 16, 473-475. doi:10.1177/1524839915580941
- Lipstein, E. A., Brinkman, W. B., Sage, J., Lannon, C. M., & DeWitt, E. M. (2013). Understanding treatment decision making in juvenile idiopathic arthritis: A qualitative assessment. *Pediatric Rheumatology*, 11, 34. doi:10.1186/1546-0096-11-34
- Lokanan, M. E. (2015). Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum*, 39, 201-224. doi:10.1016/j.accfor.2015.05.002

- Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified fisher discriminant analysis. *Expert Systems with Applications*, *42*, 2510-2516. doi:10.1016/j.eswa.2014.10.037
- Manion, R. F. (2015). Incentivizing the protection personally identifying consumer data after the Home Depot breach. *Indiana Law Journal*, *91*(1), 143-164. Retrieved from <http://ilj.law.indiana.edu/>
- Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the target data breach. *Business Horizons*, *59*, 257-266. doi:10.1016/j.bushor.2016.01.002
- Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2015). Becoming someone new: Identity theft behaviors by high school students. *Journal of Financial Crime*, *22*, 318-328. doi:10.1108/JFC-09-2013-0056
- Maroun, W., & Atkins, J. (2014). Section 45 of the auditing profession act: Blowing the whistle for audit quality? *The British Accounting Review*, *46*, 248-263. doi:10.1016/j.bar.2014.02.001
- Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interview in IS research. *Journal of Computer Information Systems*, *54*, 11-22. doi:10.1080/08874417.2013.116667
- Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage Publications.
- Martecchini, T. (2016). A day in court for data breach plaintiffs: Preserving standing based on increased risk of identity theft after Clapper v. Amnesty International

- USA. *Michigan Law Review*, 114, 1471-1496. Retrieved from <http://michiganlawreview.org/>
- McCarthy, L. A. (2016). The simultaneous experiences of being a nurse faculty member and PhD Student. *Sigma Repository*. Retrieved from <https://sigma.nursingrepository.org/handle/10755/616334>
- McDermid, F., Peters, K., Jackson, D., & Daly, J. (2014). Conducting qualitative research in the context of pre-existing peer and collegial relationships. *Nurse Researcher*, 21(5), 28-33. doi:10.7748/nr.21.5.28.e1232
- McMahon, R., Pence, D., Bressler, L., & Bressler, M. (2016). New tactics in fighting financial crimes: Moving beyond the fraud triangle. *Journal of Legal, Ethical, and Regulatory Issues*, 19(1), 16-25. Retrieved from <https://www.abacademies.org/journals/journal-of-legal-ethical-and-regulatory-issues-home.html>
- McNally, M. M. (2008). *Trial by circumstance: Is identity theft a modern-day moral panic?* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (UMI No. 3326965)
- Merriam, S. (2015). *Qualitative research: A guide to design and implementation* (4th ed). Hoboken, NJ: Jossey-Bass.
- Miller, T. W. (2017). Effectiveness of a wearable fitness tracker: Practice implications in allied health – a single case study. *Internet Journal of Applied Health Sciences and Practice*, 15(1). Retrieved from <http://nsuworks.nova.edu/ijahsp/>

- Mishra, J. S., Panda, S., & Mishra, A. K. (2013). A novel approach for credit card fraud detection targeting the Indian market. *International Journal of Computer Science Issues*, 10(3), 172-179. Retrieved from <http://ijcsi.org/>
- Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management*, 35, 21-39. doi:10.1016/j.jom.2014.10.003
- Mohammed, R. A., Wong, K. W., Shiratuddin, M. F., & Wang, X. (2018). Scalable machine learning techniques for highly imbalanced credit card fraud detection: A comparative study. In X. Geng, & B. H. Kang (Eds.), *PRICAI 2018: Trends in Artificial Intelligence. PRICAI 2018. Lecture Notes in Computer Science* (Vol. 11013). Cham, Switzerland: Springer. doi:10.1007/978-3-319-97310-4_27
- Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, 25, 1212-1222.
doi:10.1177/1049732315588501
- Moustakas, C. (1994). Chapter 6: Methods and procedures for conducting human science research. In *Phenomenological research methods* (pp. 103-120). Thousand Oaks, CA: SAGE Publications. doi:10.4135/9781412995658.d8
- Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime: The emerging threat to financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, 7, 135-143. doi:10.5901/mjss.2016.v7n3s1p135

- Mui, G., & Mailley, J. (2015). A tale of two triangles: Comparing the fraud triangle with criminology's crime triangle. *Accounting Research Journal*, 28, 45-58.
doi:10.1108/ARJ-10-2014-0092
- Murdoch, S. J., & Anderson, R. (2014). Security protocols and evidence: Where many payment systems fail. In N. Christin, & R. Safavi-Naini (Eds.), *Financial cryptography and data security. FC 2014. Lecture notes in computer science* (Vol. 8437). Berlin, Germany: Springer. doi:10.1007/978-3-662-45472-5_2
- Narang, P., Hota, C., & Sencar, H. T. (2016). Noise resistant mechanisms for the detection of stealthy peer-to-peer botnets. *Computer Communications*, 96, 29-42.
doi:10.1016/j.comcom.2016.05.017
- Nelson, J. (2016). Using conceptual depth criteria: Addressing the challenges of reaching saturation in qualitative researcher. *Qualitative Research*, 1(1), 1-17.
doi:10.1177/1468794116679873
- Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, 18, 34-35. doi:10.1136/eb-2015-102054
- Oltmann, S. M. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Information Science Faculty Publications*, 17(2), 1-16. doi:10.17169/fqs-17.2.2551
- Omar, M., Nawawi, A., & Puteh Salin, A. S. A. (2016). The causes, impact and prevention of employee fraud. *Journal of Financial Crime*, 23, 1012-1027.
doi:10.1108/JFC-04-2015-0020

- O'Reilly, M., & Parker, N. (2013). 'Unsatisfactory saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, 13, 190-197. doi:10.1177/1468794112446106
- Ortiz-Yepes, D. (2014). A critical review of the EMV payment tokenization. *Computer Fraud & Security*, (10), 5-12. doi:10.1016/S1361-3723(14)70539-1
- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42, 533-544. doi:10.1007/s10488-013-0528-y
- Patton, M. Q. (2015). *Qualitative research and evaluation methods* (5th ed). Thousand Oaks, CA: Sage.
- PCI Security Council. (2018, May). Requirements and security assessment procedure. 3.2.1, 1-139. Retrieved from https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
- Piazza, M., Fernandes, J., Anderson, J., & Olmsted, A. (2016, October). Cloud payment processing without ritualistic sacrifices reducing PCI-DSS risk surface with thin clients. *International Conference on Information Society (i-Society), Dublin, Ireland*, 166-168. Retrieved from <http://toc.proceedings.com/33439webtoc.pdf>
- 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, 9-23. doi:10.1057/s41266-017-0028-0

- Plachkinova, M., & Maurer, C. (2018). Teaching case: Security breach at Target. *Journal of Information System Education*, 29, 11-20. Retrieved from <http://jise.org/>
- Rahman, R. (2015). Comparison of telephone and in-person interviews. *Interdisciplinary Undergraduate Research Journal*, 1(1), 10-13. Retrieved from <http://knowledge.e.southern.edu/jiur/>
- Rees, J. (2014). Tackling the PCI DSS challenges. *Computer Fraud & Security*, (1), 15-17. doi:10.1016/S1361-3723(12)70009-X
- Reilly, R. C. (2013). Found poems, member checking and crises of representations. *The Qualitative Report*, 18(30), 1-18 Retrieved from <https://nsuworks.nova.edu/tqr/>
- Rennie, D. L. (2012). Qualitative research as methodical hermeneutics. *Psychological Methods*, 17, 385-398. doi:10.1037/a0029250
- Reynes, B. W., & Randa, R. (2017). Victim reporting behaviors following identity theft victimization: Results from the national crime victimization survey. *Crime and Delinquency*, 63, 814-838. doi:10.1177/0011128715620428
- Richhariyva, P., & Singh, P. K. (2014). Evaluating and emerging payment card fraud challenges and resolution. *International Journal of Computer Applications*, 107(14). Retrieved from <http://www.ijcaonline.org/>
- Rivera, J. (2018). Using the dark web to mitigate risk. *Risk Management*, 65(8), 10-11. Retrieved from <http://www.rmmagazine.com>

- Robinson, O. C. (2014). Qualitative research in psychology sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*, 25-41. doi:10.1080/14780887.2013.801543
- Robinson, N., & Aria, A. (2018). Sequential fraud detection for prepaid cards using hidden Markov model divergence. *Expert Systems with Applications, 91*, 235-251. doi:10.1016/j.eswa.2017.08.043
- Robins, C. S., & Eisen, K. (2017). Strategies for the effective use of NVivo in a large-scale study: Qualitative analysis and the repeal of *Don't Ask, Don't Tell*. *Qualitative Inquiry, 23*, 776-778. doi:10.1177/1077800417731089
- Rogers, W., & Lange, M. M. (2013). Rethinking the vulnerability of minority populations in research. *American Journal of Public Health, 103*, 2141-2146. doi:10.2105/ajph.2012.301200
- Rosaci, D., & Sarne, G. M. L. (2014). Multi-agent technology and ontologies to support personalization in B2C e-commerce. *Electronic Commerce Research and Applications, 13*, 13-23. doi:10.1016/j.elerap.2013.07.003
- Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science, 148*, 45-54. doi:10.1016/j.procs.2019.01.007
- Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach to fraud detection. *Expert Systems with Applications, 40*, 5916-5923. doi:10.1016/j.eswa.2013.05.021

- Sanjari, M., Bahramnezhad, F., Khoshnava Foman, F., Shogi, M., & Ali Cheraghi, M. (2014). Ethical challenges of researchers in qualitative studies: The necessity to develop a specific guideline. *Journal of Medical Ethics & History of Medicine*, 7, 1-6. Retrieved from <http://jmhm.tums.ac.ir>
- Saravanan, S. K., & Suresh Babu, G. N. K. (2017). Secured credit card transaction using MCOP. *Journal of Internet Banking and Commerce*. Retrieved from <http://www.icommercecentral.com/open-access/secured-credit-card-transaction-using-mcop.php?aid=86181>
- Sari, A., & Karay, M. (2015). Comparative analysis of wireless security protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*, 8, 483-491. doi:10.4236/ijcns.2015.812043
- Seeja, K., & Zareapoor, M. (2014). Fraudminer: A novel credit card detection model based on frequent itemset mining. *The Scientific World Journal*. doi:10.1155/2014/252797
- Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information*, 32, 314-341. doi:10.1080/074212222015.1063315
- Schuchter, A., & Levi, M. (2015). Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum*, 39, 176-187. doi:10.1016/j.accfor.2014.12.001
- Shaw, D. M., & Erren, T. C. (2015). Ten simple rules for protecting research integrity. *PLoS Computational Biology*, 11(10). doi:10.1371/journal.pcbi.1004388

- Shapka, J. D., Domene, J. F., Khan, S., & Yang, L. M. (2016). Mobile customer relationship management: A competitive tool. *EXCEL International Journal of Multidisciplinary Management Studies*, 4(7), 37-42. Retrieved from <http://www.zenithresearch.org.in/index.php/journals-information/92-eijmms.html>
- Simon, S., & Cagle, C. (2017). Culture's impact on trust, distrust, and intentions in data theft environments: A cross-cultural exploratory study. *Journal of Global Information Technology Management*, 20, 214-235. doi:10.1080/1097198X.2017.1388672
- Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *The Qualitative Report*, 21(2), 376-392. Retrieved from <https://nsuworks.nova.edu/tqr/>
- Sinha, S., & Yadav, R. S. (2017). Workplace bullying in school teachers: An Indian inquiry. *Indian Journal of Health and Wellbeing*, 8(3), 200-205. Retrieved from http://www.iahrw.com/index.php/home/journal_detail/19#list
- Small, M. (2014). From data breach to information stewardship. *Network Security*, (10), 5-8. doi:10.1016/S1353-4858(13)70112-0
- Steer, J. (2014). The gaping hole in our security defences. *Computer Fraud & Security*, (1), 17-20. doi:10.1016/S1361-3723(14)70009-0
- Sullivan, R. J. (2013). The U.S. adoption of computer-chip payment cards: Implications for payment fraud. *Economic Review*. Retrieved from <https://www.kansascityfed.org/PUBLICAT/ECONREV/PDF/13Q1Sullivan.pdf>

- Suman, R. (2014). Analysis on credit card fraud detection models. *International Journal of Computer Trends and Technology*, 8(1), 45-51. Retrieved from <http://www.ijctjournal.org>
- Tan, F. T. C., Guo, Z., Cahalane, M., & Cheng, D. (2016). Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution. *Information Management*, 53, 878-891. doi:10.1016/j.im.2016.07.002
- Tatham, M. (2018). *Identity theft statistics*. Retrieved from <https://www.experian.com/blogs/ask-experian/identity-theft-statistics/>
- Topkaya, N. (2015). Factors influencing psychological help seeking in adults: A qualitative study. *Educational Sciences: Theory and Practice*, 15(1), 21-31. Retrieved from <http://www.estp.com/tr>
- Tran, V., Porcher, R., Ravaud, P., & Falissard, B. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, 80, 88-96. doi:10.1016/j.jclinepi.2016.07.014
- Trustwave. (2016). *Executive summary: Trustwave global security report*. Retrieved from <https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf>
- Turley, E. L., Monro, S., & King, N. (2016). Doing it differently: Engaging interview participants with imaginative variation. *Indo-Pacific Journal of Phenomenology*, 16, 153-162. doi:10.1080/20797222.2016.1145873

- Turner, L. (2010). "Medical tourism" and the global marketplace in health services: U.S. patients, international hospitals, and the search for affordable healthcare. *International Journal of Health Services*, 40, 443-467. doi:10.2190/HS.40.3.d
- Turner, M. J. (2014). An investigation of big five personality and propensity to commit white collar crime. In D. B. Schmitt (Ed.), *Advances in accounting behavioral research (Advances in Behavioral Research)* (Vol. 17, pp. 57-94). Bingley, United Kingdom: Emerald Group Publishing. doi:10.1108/S1475-148820140000017002
- United States Government Accountability Office. (2014). *Testimony before the committee on Homeland Security and Governmental affairs. United States Senate. Information Security Federal Agencies need to enhance responses to data Breaches*. Washington, DC. Retrieved from <http://www.gao.gov/assets/670/662227.pdf>
- U.S. Department of Health and Human Services, Office of the Secretary, The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Washington, DC. Retrieved from <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html>
- Vaishali, V. (2014). Fraud detection in credit card by clustering approach. *International Journal of Computer Applications*, 98(3), 29-32. doi:10.5120/17164-7225

- Vaitkevicius, S., & Kazokiene, L. (2013). The quantitative content processing methodology: Coding of narratives and their statistical analysis. *Engineering Economics, 24*, 28-35. doi:10.5755/j01.ee.24.1.2350
- Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems, 75*, 38-48. doi:10.1016/j.dss.2015.04.013
- van Zyl, H. J., Bam, W. G., & Steenkamp, J. D. (2016). Identifying barriers faced by key role players in the South African manganese industry. *27th Annual SAIIE Conference, Stonehenge South Africa*, 365-375. Retrieved from <http://repository.nwu.ac.za>
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide. Guidelines for conducting mixed methods research in information systems. *Management Information Systems Quarterly, 37*, 21-54. Retrieved from <http://www.misq.org>
- Vogl, S. (2013). Telephone versus face-to-face interviews mode effect on semistructured interviews with children. *Sociological Methodology, 43*, 133-177. doi:10.1177/0081175012465967
- Vojir, T., Matas, J., & Noskova, J. (2016). Online adaptive hidden Markov model for multi-tracker fusion. *Computer Vision and Image Understanding, 153*, 109-119. doi:10.1016/j.cviu.2016.05.007

- Vona, L. W. (2015). *Fraud risk assessment: Building a fraud audit program*. Hoboken, NJ: John Wiley & Sons. doi:10.1002/9781119196655.ch14
- Wang, F., Chang, C. C., & Lyu, W. L. (2015). The credit card visual authentication scheme based on GF(2⁸) field. *Multimedia Tools and Applications*, 74, 11451-11465. doi:10.1007/s11042-014-2238-1
- Wang, T. S., Lin, H. T., Cheng, W. T., & Chen, C. Y. (2017). DBod: Clustering and detecting DGA-based botnets using DNS traffic analysis. *Computers & Security*, 64, 1-5. doi: 10.1016/j.cose.2016.10.001
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers and Security*, 57, 47-66. doi:10.1016/j.cose.2015.09.005
- Willey, L., & White, B. J. (2013). Do you take credit cards? Security and compliance for the credit payment industry. *Journal of Information Systems Education*, 24(3), 181-188. Retrieved from <https://aisel.aisnet.org/jise/>
- Williamson, I., Leeming, D., Lyttle, S., & Johnson, S. (2015). Evaluating the audio diary method in qualitative research. *Qualitative Research Journal*, 15, 20-34. doi:10.1108/QRJ-04-2014-0014
- Wilson, E. (2019). Disrupting dark web supply chains to protect precious data. *Computer Fraud & Security*, (4), 6-9. doi:10.1016/S1361-3723(19)300-39-9
- Whitler, K. A., & Farris, P. W. (2017). Impact of cyber-attacks on brand image. *Journal of Advertising Research*, 3-9. doi:10.2501/JAR-2017-005

- Wolf, L. E., Patel, M. J., Williams Tarver, B. A., Austin, J. L., Dame, L. A., & Beskow, L. M. (2015). Certificate of confidentiality: Protecting human subject research data in law and practice. *Journal of Law, Medicine, & Ethics*, *43*, 594-609.
doi:10.1111/jlme.12302
- Xu, W. M., & Storr, G. B. (2013). Learning the concepts as instrument in qualitative research. *The Qualitative Report*, *17*, 1-18. Retrieved from
<http://nsuworks.nova.edu/tqr/>
- Yelland, M. (2013). Fraud in mobile in networks. *Computer Fraud & Security*, (3), 5-9.
doi:10.1016/S1361-3723(13)70027-7
- Yin, R. K. (2009). *Case study research: Designs and methods* (4th ed.). Los Angeles, CA: Sage.
- Yin, R. K. (2014). *Case study research: Designs and methods* (5th ed.). Los Angeles, CA: Sage.
- Yulianto, S., Lim, C., & Soewito, B. (2016). Information security maturity model a best practice driven approach to PCI DSS compliance. *2016 IEEE Symposium*, 65-70.
Retrieved from <https://ieeexplore.ieee.org/document/7519379>
- Zohrabi, M. (2013). Mixed method research: instruments, validity, reliability, and reporting findings. *Theory and Practice in Language Studies*, *3*, 254-262.
doi:10.4304/tpls.3.2.254-262

Appendix A: Explanation of Card Stripes Track 1

Track 1 Data Structure		
<i>Field Name</i>	<i>Length</i>	<i>Comments</i>
Start Sentinel (SS)	1 character	Indicates the beginning of Track 1; set to "%"
Format Code (FC)	1 character	Indicates the card type; "B" indicates a credit/debit card
Primary Account Number (PAN)	up to 19 digits	Always numerical; usually set to the credit/debit card number
Field Separator (FS)	1 character	Delimits Track 1 fields; set to "^"
Name	2-26 characters	Account holder's name
Field Separator (FS)	1 character	Delimits Track 1 fields; set to "^"
Expiration Date (ED)	4 digits	Always in the format YYMM
Service Code (SC)	3 digits	Indicates what types of charges can be accepted
Discretionary Data (DD)	Variable*	Determined by card issuer--may include Card Code and/or PINs
End Sentinel (ES)	1 character	Indicates the end of Track 1; set to "?"
Longitude Redundancy Check (LRC)	1 character	Used to verify that Track 1 was read accurately

Note * Track 1 Data cannot exceed 79 characters, including all Sentinels, Field Separators, and the LRC. The length of Discretionary Data is restricted as a result and tends to hold relatively low values. Adapted from

<https://support.authorize.net/authkb/index?page=content&id=A755>

Appendix B: Explanation of Card Stripes Track 2

The format for Track 2 Data was developed by the American Banking Association (ABA) and tends to be much shorter and holds less information:

Track A2 Data Structure		
<i>Field Name</i>	<i>Length</i>	<i>Comments</i>
Start Sentinel (SS)	1 character	Indicates the beginning of Track 2; set to ","
Primary Account Number (PAN)	up to 19 digits	Always numerical; usually set to the credit/debit card number
Field Separator (FS)	1 character	Delimits Track 2 fields; set to "="
Expiration Date (ED)	4 digits	Always in the format YYMM
Service Code (SC)	3 digits	Indicates what types of charges can be accepted
Discretionary Data (DD)	Variable*	Determined by card issuer--may include Card Code and/or PINs
End Sentinel (ES)	1 character	Indicates the end of Track 2; set to "?"
Longitude Redundancy Check (LRC)	1 character	Used to verify that Track 2 was read accurately

Note * Track 2 Data cannot exceed 40 characters, including all Sentinels, the Field Separator, and the LRC. The length of Discretionary Data is restricted as a result and tends to hold relatively low values. Adapted from <https://support.authorize.net/authkb/index?page=content&id=A755>

Appendix C: Cover Letter

January 23, 2019

Doctoral Candidate

[REDACTED]
[REDACTED]
[REDACTED]

404-747-1304

CC/BCC Block: Dr. Diane Dusick, Chair

Enclosure: 2

charles.ross2@waldenu.edu

Dear [REDACTED]

I am writing to you to inquire about performing a research project with [REDACTED] and the Information Technology department. I am an on-online doctoral student at Walden University in Minneapolis, Minnesota working on my dissertation. My dissertation is entitled "Reducing or Eliminating Payment Card Fraud".

I am requesting your permission to interview your data security/network security personnel to determine what other companies can do in the future to reduce or eliminate card fraud. I have enclosed sample questions and a permission form for your perusal and approval. I have to wait for Walden's IRB approval however to move forward with the interviews. The interviews would be conducted off-site and after normal business hours.

Thanks for your consideration.

Charles Ross

Appendix D: Consent Form

TITLE OF STUDY

Reducing or Eliminating Payment-Card Fraud

PRINCIPAL INVESTIGATOR

Charles Ross

Doctoral Candidate Business Administration – Social Impact Management

2817 Muscadine Dr, Augusta, GA 30909

404-747-1304

charles.ross2@waldenu.edu

PURPOSE OF STUDY

You are being asked to take part in a research study. Before you decide to participate in this study, it is important that you understand why the research is being done and what it will involve. Please read the following information carefully. Please ask the researcher if there is anything that is not clear or if you need more information.

The purpose of this study is to explore the beliefs, understandings, and perceptions of payment-card acceptors about security strategies that would reduce or eliminate identity theft and reduce or eliminate payment-card fraud. The results of the research will contribute to data-security specialist strategies in reducing and or eliminating financial loss from payment-card fraud via the Internet, or brick and mortar retail locations through enhancing payment-card security strategies within the retail industry of the United States. The interviews would be held off-site at a local coffee shop or mutually agreed upon location where both parties feel comfortable and safe.

STUDY PROCEDURES

If you agree to be in this study, you will be asked to

- Participate in audio recorded face to face interviews lasting approximately 60 to 90 minutes
- Follow up interviews may occur to ensure accuracy and clarity of interviewee responses lasting approximately 60 minutes

Here are some sample questions:

1. Technology-wise, there are different ways for card acceptors to combat fraud. What technology tools has your organization implemented?
2. How effective are the tools your organization implemented?
3. PCI-DSS standards are minimal at best. What changes do you believe, need to occur to the standards that could increase security?
4. What have you implemented to make your payment-card strategy stronger and yet less costly for your company?

RISKS

Psychological distress – refers to the emotional and physiological reactions experienced when an individual confronts a situation in which the demands go beyond their coping resources. Examples of stressful situations are marital problems, death of a loved one, abuse, health problems, and financial crises - minimal risk.

Relationship harm – Difficult situations dealing with other people (communication, relationship, etc.) (*Interpersonal*) may become a stressor when it is perceived as a threat to one's well-being or position in life - minimal risk.

Legal – the minimal risk for litigation, breach of contract, or regulatory for everyday business and interactions – minimal risk.

Economic loss – Economic loss may mean someone losing a job however, the researcher doubts anyone would lose their position due to the discussion – minimal risk

Professional reputation – minimal risk.

Physical harm – Physical harm is not a consideration at this time as the person will not be put into a position to harm themselves or consider inflicting harm to anyone -- minimal risk

You may decline to answer any or all questions and you may terminate your involvement at any time if you choose.

BENEFITS

There will be no direct benefit to you for your participation in this study. However, we hope that the information obtained from this study may provide a foundation

for strategies businesses can use to reduce and or eliminate payment-card fraud through improved fraud detection strategies.

CONFIDENTIALITY

For the purposes of this research study, your comments will not be anonymous. Every effort will be made by the researcher to preserve your confidentiality including the following:

- Assigning code names/numbers for participants that will be used on all research notes and documents
- Keeping notes, interview transcriptions, and any other identifying participant information in a locked file cabinet in the personal possession of the researcher.

Participant data will be kept confidential except in cases where the researcher is legally obligated to report specific incidents. These incidents include, but may not be limited to, incidents of abuse and suicide risk.

COMPENSATION

There will be no monetary compensation for participating in the study. The study is completely voluntary

CONTACT INFORMATION

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via Charles Ross at 404-747-1304 or via e-mail charles.ross2@waldenu.edu or nissankid@yahoo.com. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is **IRB will enter approval number here** and it expires on **IRB will enter an expiration date.**

VOLUNTARY PARTICIPATION

Your participation in this study is voluntary. It is up to you to decide whether or not to take part in this study. If you decide to take part in this study, you will be asked to sign a consent form. After you sign the consent form, you are still free to withdraw at any time and without giving a reason. Withdrawing from this study will not affect the

relationship you have, if any, with the researcher. If you withdraw from the study before data collection is completed, your data will be returned to you or destroyed.

CONSENT

I have read, and I understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntarily agree to take part in this study. You may print a copy of this form for your records.

Participant's signature _____ Date _____

Investigator's signature _____ Date _____

Appendix E: Interview Protocol

- I. Introduce myself to participants
- II. Present consent form, review consent form, answer any questions, address any concerns of the participants
- III. Have participant sign consent form
- IV. Present Confidentiality Agreement, answer any questions, address any concerns of the participants
- V. Give a copy of consent form to participant
- VI. Turn on the recording device
- VII. Follow procedure to introduce participants with coded identification, note date and time
- VIII. Begin the interview with Question 1, follow through to the final question
- IX. Follow up with additional questions
- X. End interview sequence; discuss member checking with participants
- XI. Thank the participants for their part in the study. Reiterate contact information for follow up questions and concerns
- XII. End protocol

Appendix F: Interview Questions

Project: Walden University Doctoral Study

Type of Interview

Date:

Place:

Interviewer:

1. What opportunities still exist for a person to commit payment-card fraud at the card processing level?
2. What legal strategies do you see organizations taking to protect themselves from financial loss from data breaches?
3. What plans do you have to implement payment-card security?
4. How has your organization increased security to reduce those opportunities?
5. There are different ways for card acceptors to combat fraud. What technology tools has your organization implemented?
6. What strategies have you implemented or planning to make your payment-card protection strategy stronger and yet less costly for your company?
7. How effective are the tools and strategies your organization has implemented?
8. What changes in the PCI-DSS standards need to be added that could increase security?
9. What steps can payment-card acceptors take to increase security for accepting payment cards?
10. If you implemented fraud-detection practices, what problems did you encounter during the conversion?
11. What else can you add regarding strategies that the payment-card acceptors could implement to reduce and eliminate fraud and identity theft?

Notes: