8-2016

The Forgotten Signature: An Observational Study on Policy of Securing Identity in Prevention of Identity Theft and Credit/Debit Card Fraud at Retail Store POS Terminals

Belinda R. Wilson
East Tennessee State University

The Forgotten Signature: An Observational Study on Policy of Securing Identity in Prevention of Identity Theft and Credit/Debit Card Fraud at Retail Store POS Terminals

---

A thesis

presented to

the faculty of the Department of Criminal Justice and Criminology

East Tennessee State University

In partial fulfillment

of the requirements for the degree

Masters of Arts in Criminal Justice and Criminology

---

by

Belinda R. Wilson

May 2016

Dr. Larry Miller, Chair

Dr. John Whitehead

Dr. Chris Rush

Keywords: Identity Theft, Credit/Debit, Bank Card, POS Terminal, EMV, Capable Guardian, FDE, R.A.T.-Routine Activities Theory

ABSTRACT

The Forgotten Signature: An Observational Study on Policy of Securing Identity in Prevention of Identity Theft and Credit/Debit Card Fraud at Retail Stores 'POS Terminals

by

Belinda R. Wilson

Identity theft and credit and bank card fraud is increasing in America and worldwide. Given the current statistics of its prevalence and practices around the world, many in government are starting to take critical notice due to its impact on a nation's economy. Limited amounts of research have been conducted regarding the practices of applying the Routine Activities Theory (Cohen & Felson, 1979) to better equip store managers in understanding the critical need for capable and effective point of sale guardianship for in-store prevention of credit or bank card fraud due to identity theft. This research has used qualitative observational studies to investigate the presence of or lack of capable guardianship at point of sales transactions in large department stores where a majority of in-store credit and bank card fraud loss occurs. Findings conclude an overwhelming lack of capable guardianship at retail store POS terminals.

DEDICATION

The author wishes to dedicate her work in memory of her beloved deceased grandmother, Ruth Hydle, who taught her critical life skills, including money management as an adolescent; and, in memory of Jewel Edward Wilson, her deceased veteran father, who served in Vietnam as a military police officer. He taught her to be continually keenly aware of her surroundings in the world around her and strive to maintain safety for herself and others. May their souls rest in peace.

ACKNOWLEDGEMENTS

The author would like to especially thank the members of her Graduate thesis committee, Dr. Larry Miller, Chair, and Dr. John Whitehead for all of their assistance and support during this project and throughout her career at East Tennessee State University. Special thanks goes out to Dr. Chris Rush for her substitution as committee member, after the retirement of Dr. Dennis Hamm. Thank you, Dr. Hamm, for your insight in research development and for encouraging me to pursue a topic in research pertaining to a prevalent and relevant issue in today's society: Identity theft and card fraud.

The author would also like to express deep appreciation to her children, Corey Wilson, Gracie Wilson, and Ariel Courtney, for their continued love, support and patience for many long years, while she completed her studies and research as a single parent. Special thanks goes out to supporting family members: Vicky Wilson, for her prayers, love and faithful support in many ways; Shirley Rainwater, for her faith, love and care; Chris and Sandra Beam, for their care for the author's "handicap-able" son, Corey, and teenage daughter, Gracie, during the author's studies abroad throughout her career at E.T.S.U.

Above all, the most gratitude possible is extended to the author's Lord and Savior, Jesus Christ, who gave her daily strength to become the first college graduate in her family, setting a precedent for future generations to follow.

TABLE OF CONTENTS

Page

ABSTRACT 2

DEDICATION 4

ACKNOWLEDGEMENTS 5

LIST OF TABLES 10

Chapter

1. INTRODUCTION 11

Statement and Significance of the Problem 12

Purpose of this Research 18

Research Questions Addressed and Hypotheses 19

Limitations of the Study 22

Definition of Terms 23

2. LITERATURE REVIEW 39

Theory 39

Credit Card Fraud 41

Intertwined Problem of Identity Theft 42

Empirical Studies and Research Explaining Identity Theft 43

Effects of Identity Theft on Card Users 50

The Challenge of Capable Guardianship 52

The Places a Consumer is at Risk 55

Outdoor Terminals 56

Restaurants 56

Online....57
Retail Stores....61
Summary of Literature Review....65
3. METHODOLOGY....66
Purpose of Research Restated....66
Review of Research Questions Addressed and Hypotheses....67
Procedures for Collecting Data....70
Store Chains and Coding....71
Participants at POS Terminals....72
Purchases....73
Payment Methods and Security Features of Cards Used....74
Construction of Observations Report....74
Coded Chain Store Locations and Numbers (#)....75
Time Segments Transactions Occurred....75
Demographics of Participants at POS Terminals....76
Location of POS Terminal within Stores....77
Electronic vs. Non-Electronic Items....77
Amount of Charges to Specific Card Used....78
Card Being Used for Transaction and Coding....78
Guardianship Efforts of Participant Employees....79
Technology Used in Transactions....80
Additional Notes and Observations....81

4. RESEARCH FINDINGS 82
Distribution of Store Chains 83
Distribution of Participants 83
Distribution of POS Terminals 86
Purchases and Data Analysis Strategy 86
Credit Card Data Analysis and Coding 93
Summary of Transactions 97
Findings on Guardianship Efforts by Participants at POS Terminals 103
Research Question 1 Findings and Hypothesis Discussed 103
Research Question 2 Findings and Hypothesis Discussed 106
Research Question 3 Findings and Hypothesis Discussed 107
Research Question 4 Findings and Hypothesis Discussed 108
Research Question 5 Findings and Hypothesis Discussed 108
5. DISCUSSIONS 110
Summary of Findings 111
Conclusions 113
Limitations of Thesis Research 114
Recommendations 115
Future Research 116
REFERENCES 117
APPENDICES 123
Appendix A: Observations Report 123

Appendix B: Bank Card Rules and Regulations 124

Appendix C: Visa Rules for Unsigned Cards 126

Appendix D: MasterCard Rules for Unsigned Cards 128

VITA 129

LIST OF TABLES

Table Page

1. Region of Coded Store Chains Patronized for Observational Studies....84

2. Demographics and Numbers of Participants....86

3. POS (Point of Sale) Terminal Locations within Stores Utilized for Face-to-Face Transactions....87

4. Time Segments when Purchases Were Made....90

5. Itemized List of 34 Purchases, Charges Incurred, and Technology Used for Transaction....91

6. Electronics Related Purchases vs. Non-Electronics Related Purchases....94

7. Total Charges Incurred at Each Store for All 34 Transactions....98

8. Number of Sales Transactions Attributed to Each Card....99

9. Test Question 1 Results for Analyzing Capable Guardianship....101

10. Test Question 2 Results for Analyzing Capable Guardianship....101

11. Test Question 3 Results for Analyzing Capable Guardianship....102

12. Test Question 4 Results for Analyzing Capable Guardianship....102

13. Results of Accumulative %'s of All Test Questions Combined for Analyzing Capable Guardianship....103

14. Variates 1 & 2 in Demographics' Effects on Presence of Capable Guardianship....104

15. Variates 3, 4, & 5's Effects on Presence of Capable Guardianship....105

CHAPTER 1

INTRODUCTION

Identity theft and bank card fraud has been on the rise in America and worldwide. According to the United States Department of Justice, Bureau of Justice Statistics, there were 17.6 million U.S. residents who reported experiencing identity theft in 2014 alone (Harrell, 2015). Surprisingly, two-thirds of these suffered direct financial loss of $99 or less that involved fraudulent plastic card purchases. Accumulatively, "direct and indirect losses from identity theft totaled $24.7 billion in 2012" (Harrell, 2013). Considering the crime is a white collar financial crime, it is relatively difficult to assess and most difficult to research and analyze. Given the current statistics of its prevalence and practices around the world, many in government are starting to take critical notice due to its impact on a nation's economy. Some researchers have attempted to understand this phenomena by applying certain criminological theories to their research (Hollis, Felson, & Welsh, 2013; Tillyer & Eck, 2011; White & Fisher, 2008). However, extremely limited amounts of research have been conducted regarding the practices of applying the Routine Activities Theory (Cohen & Felson, 1979) to better equip store managers in understanding the critical need for capable and effective point of sale guardianship for in-store prevention of credit or bank card fraud due to identity theft (Masuda, 1992; Sampson, Eck, & Dunham, 2008; Vaughan, 1998). This research has explored the absence or presence of capable guardianship at point of sales in large department stores where a majority of in-store identity theft and plastic card fraud loss occurs.

Statement and Significance of the Problem

According to a U.S. Department of Justice report explaining criminal fraud, in 1998, Congress created a new federal offense called "identity theft." This new federal offense was a result of an infamous case of identity theft where a convicted felon had incurred more than $100,000 of credit card debt in the name of is victim. The identity thieve purchased homes, handguns, motorcycles and other costly items before filing for bankruptcy—also in his victim's name (U.S. Dept. of Justice, 2015). Since that first label identifying 'identity theft,' a more recent publication, *Victims of Identity Theft, 2012* Bureau of Justice Statistics reported that "the majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit and debit card or bank account information" (Harrell & Langton, 2013). According to this same report, "direct and indirect losses from identity theft totaled $24.7 billion in 2012," in the U.S. alone (Harrell & Langton, 2013). Identity theft and credit or debit forms of plastic card fraud accounted for over 800 million English pounds worth in fraud loss worldwide several years ago. This figure translated to be approximately $1550 million in US currency at previous exchange rates (Gee et al., 2010 as cited in Papadopoulos and Brooks, 2011). It was reported by other researchers that more than 27 million Americans were victims of identity theft and fraud just within five previous years combined (Gerard, Hillison, & Pacini, 2004 as cited in White & Fisher, 2008). The numbers have escalated since. In 2014 alone, an "estimated 17.6 million persons, or 7% of all U.S. residents age 16 or older, were victims of one or more incidents of identity theft," up from the 16.6 million persons reported in 2012 (Harrell, 2015). It was also reported that "in 2014, the most common type of identity theft was the unauthorized misuse or attempted misuse of an existing account and that of those about 79% of

victims experienced a single incident of identity theft, while 21% experienced multiple incidents" (Harrell, 2015).

Financial identity theft and fraud occurs when identity thieves use a victim's personal identifying information to conduct fraudulent financial practices that include drawing money from a victim's bank account, opening up a new bank account or other line of credit in the victim's name, or stealing the victim's personal identifying information for specific purposes of creating fake credit cards using the name of the victim—all the while he or she still holds the card in hand (White & Fisher, 2008). Identity theft and credit card fraud can occur online or in-store and without the victim's awareness, until after the loss has incurred and their account has been damaged. When this happens, the victim has the primary responsibility of discovering it and reporting to their bank institution or credit card company. They in turn attempt to refund the loss, while re-distributing the costs of the loss onto the customers. There is a critical window of opportunity for the victim to report the loss in order to minimize it—the first 48-72 hours that his or her card is being fraudulently charged. If a customer gets notice 30 days later when the bill arrives in the mail, it may be too late to stop the account from having been drained or the credit card from having been completely maxed out.

Both in-store and online identity theft and credit fraud is on the increase. Most research has been done on the themes of absence of capable guardianship and the victimization of suitable online targets using the routine activities theory (Bossler & Holt, 2009; Choo, 2011; Holtfreter, Reisig, & Pratt, 2008; Kleemans, Soudijn, & Weenink, 2012; Pratt, Holtfreter, & Reisig, 2010; Reyns, 2010). One study used integrated theory of Routine Activities Theory (Cohen & Felson,1979) and Lifestyle Exposure Theory (Hindelang, Gottfredson, & Garofalo, 1978) to conduct an empirical assessment of 204 college students in hopes to gain an overall picture of the

relationship between the causal factors and online victimization (Choi, 2008). According to Choi online computer crimes such as these are rarely detected by the victims or reported to the police (Choi, 2008, p. 308). Accounts can be hacked into without the victim's knowledge until it is too late. "Hacking" refers to the unauthorized access with intent to cause damage, steal property (databases containing customers' account information) and leaving behind some evidence of a successful break-in (National White-Collar Crime Center 2003, p.1 as cited in Choi, 2008). White collar crimes are particularly hard to research and prosecute because it is difficult to discover the faceless motivated offenders. So the need for adequate guardianship is primary to avoid the attack and the fraud loss incurred. According to Choi, the crucial key purpose of capable guardianship online as well as in real life is to *prevent* crime (Choi, 2008). The results from his empirical assessment demonstrated that the online lifestyle and digital guardianship are important aspects of computer crime victimization (Choi, 2008, p. 325). Other research studies analyze online statistical fraud detection systems and have been conducted around the world in countries such as Australia, Turkey, Korea, and America (Bolton & Hand, 2002; Choo, 2011; Duman & Ozcelik, 2011; Lee, Cho, Chae, & Shim, 2009). The problem is that the statistical detection systems are only useful after the identity theft and plastic card fraud has already occurred and damages have incurred. By this time, money has been lost and crime has prevailed. There is currently nothing available in research demonstrating technology that is capable of acting as a completely reliable and adequate guardian to prevent online or in-store identity theft and fraud loss. The software available is only capable of detecting the fraud once it has happened—and that only part of the time. This lack of adequate technological guardianship has given cause for the rise of more sophisticated security measures being placed upon the plastic card payment form itself. Hence, the EMV chip technology, or European Model Visa

card security measures have recently been implemented into the United States. As of October 1, 2015 the EMV liability shift has changed the face of how merchants are doing business in their daily routine activities of accepting Visa and MasterCard plastic card payments. Visa and MasterCard were amongst the first of all credit card companies to make the transition of encrypting EMV chip technology into their cards produced for customers residing within the United States. Along with this new technology, comes the accountability of merchants for accepting fraudulent card payments. The merchants and their employees are now being held liable and responsible for all chargebacks and fraud loss, rather than the credit card companies themselves. This new EMV liability shift has required a transition from old equipment at in-store POS terminals to be replaced by new equipment that has capabilities of reading the EMV chip encrypted into the new cards. Due to a backlog of reader approvals and certifications, as well as the costly transfer of equipment, many merchants are still in the process of making the mandated transition. Meanwhile, magnetic stripes are still located on the backs of each of the cards that are containing the new encrypted EMV chip technology and those strips still contain all of the account holders' personal identifying information and can still be skimmed by devices that read magnetic strips. Many merchants are still using the swipe method of reading the magnetic strips to process the transactions at the in-store POS terminals while awaiting certification of their new equipment. This leads to this thesis paper's initial research question of current absence or presence of capable guardianship being demonstrated by merchants and their employees at their in-store POS terminals.

Only limited research has currently been done on the absence of capable guardianship regarding in-store purchases (Hollis et al., 2013; Sampson et al., 2010; Tillyer & Eck, 2011). Some have applied routine activities theory in attempts to understand how to get a handle on

crimes involving fraud. Others have tried to analyze trends to build a defense (Prabowo, 2011). One particular study attempts to analyze the prevalence, clearance rates, and victim/offender characteristics (Allison, Schuck, & Lersch, 2005). Very limited research has been done on actual identity theft and credit card fraud prevention itself (Anderson, Durbin, & Salinger, 2008; Barker, D'Amato, & Sheridon, 2008). A few other studies conducted are relative to the topic of handlers and managers and raising their guardianship capabilities and accountabilities (Masuda, 1992; Sampson et al., 2010; Vaughan, 1998). However, the only current study done within the past decade is that of Sampson et al., (2010) applying routine activity theory to explain crime prevention success or failure. This study is an important study to the to the topic of why and how in-store point of sales transactions are critical junctures of catching identity thieves and credit card fraudsters by holding the managers liable as "super controllers for crime prevention" (Sampson et al., 2010). A final relevant study to the topic of in-store identity theft and credit card fraud can be found in an article published by *Journal of Business Research,* entitled "Repercussions of promoting an ideology of consumption: Consumer misbehavior" (Fullerton & Punj, 2004). This article describes consumer misbehaviors coming in many forms such as shoplifting, vandalism, credit card fraud, and physical or verbal abuse of other consumers and of marketer employees (Fullerton & Punj, 2004). Due to these consumer misbehaviors, it is suspected that many businesses would prefer to chalk fraud loss up to the costs of doing business rather than jeopardize employees' safety or allow credit card fraudsters to create an atmosphere of disharmony within the store and frighten other customers causing the store to lose their business.

Policy making and policing of identity theft and credit and bank card fraud present additional challenges. According to research, 40% of it goes unreported to police authorities

(Papadopoulos & Brooks, 2011; White & Fisher, 2008). There is a call for new public management for policing of fraud (Doig, Johnson, & Levi, 2001). There is also a need for offender-based research to inform policy on adequate guardianship prevention methods (Copes & Vieraitis, 2009; Copes, Veiratis, & Jochum, 2007). As previously discussed, new changes in policy have been made by Visa and MasterCard regarding the EMV liability shift that took place beginning October 1, 2015. But those policy changes in credit card companies alone, even with the new EMV chip card encryptions, are questionably inadequate in handling the job of policing this crime or preventing it, which became inherently evident during the field research and observational studies accumulated for this thesis.

Based upon the review of the most available material on this topic of research, it is apparent there is a need for redefining capable guardianship. As demonstrated through various applications to the many elements surrounding identity theft and plastic card fraud, it is warranted that routine activities theory (Cohen & Felson, 1979; Felson, 2008; Felson & Clarke, 1998) is the most applicable criminology theory for explaining this phenomenon. The absence of capable guardianship prevails over fraudulent plastic card transactions and demonstrates dire need of research in efforts of understanding the problem and why there is such negligence. This research is necessary as serious study for developing future policies for creating a presence of capable guardianship in order to more effectively deter and prevent this crime. The dominant themes throughout the body of research materials has covered various aspects relating to routine activities theory regarding motivated offenders and suitable targets, yet it has minimally addressed the reasoning of why there is absence of capable guardianship when customers pay with plastic cards. This absence of capable guardianship has allowed identity theft and plastic

card fraud crimes to continue to grow by leaps and bounds—both within the cyber world and the real physical world.

Purpose of this Research

The purpose of this research is to investigate by first-hand field observations the absence or presence of capable guardianship at point-of-sale (POS) terminals within retail store chains that are known to be highly targeted for identity theft in conjunction with credit, debit or bank card fraud. (See pages 61- 62 of this thesis). A majority of bank cards bear the logo of either Visa or MasterCard. Both Visa and MasterCard mandate certain rules and regulations to be followed by merchants and their employees as outlined by their merchant agreement contracts (See Appendices C & D). Banks also have their own specific rules and regulations that are to be adhered to in order for the merchant to accept the card bearing the Visa or MasterCard logo for payment (See Appendix B).

Specifically, these rules require that each card must bear the legal cardholder's genuine signature on the back of the card within the signature strip that is located below the magnetic strip and beside the CVV code. Either above or below each signature strip located on the back of each card, are the words that read, "AUTHORIZED SIGNATURE – NOT VALID UNLESS SIGNED" (See Appendix C). Point-of-sale face-to-face transactions that occur within retail stores, with cards in hands of customers, are considered by both Visa and MasterCard to be the least risky transactions of all because the merchant's employees have the opportunity to investigate the identity of the customers paying with a plastic card method, and are required to do so if the card is not signed. The steps that the employees must follow at the POS terminal during the transaction are outlined by Bank Rules, Visa, and MasterCard (See Appendices B, C, & D for details). This investigator believes that the responsibility of acting as a capable guardian

that is placed upon the merchant and its employees is one that is often neglected and dismissed, thus it is also a contributing factor to the increase of identity theft related to card fraud.

Research Questions Addressed and Hypotheses

Specifically, the following questions were addressed and hypothesized:

RQ1: The first research question contains five parts: 1) Will the cashier at the point of sale transaction act as a capable guardian over the face-to-face transaction and act to help prevent identity theft and credit/debit card fraud by taking the card into his or her hand to visually check the back of the credit or debit card to see if it bears an authorized signature by the legal cardholder, or check the account number on the card and compare it to that in the system or receipt in according to the merchant agreement rules as mandated by the Bank Rules and Regulations, Visa and MasterCard? (See Appendices B, C, & D). Variables investigated: 2) Will the variables of non-electronic versus electronic purchase increase levels of capable guardianship? Will there be a difference in the level of capable guardianship if the purchase is made at the back electronic counter POS terminal versus the store's front end POS terminal? 3) Will the higher amount of purchase charges to the card raise levels of guardianship at POS terminals with electronic purchases compared to a low levels of guardianship for small charges to the card? 4) Will the variables of time segment of day or night and business or lack thereof give increase or decrease to the levels of capable guardianship? 5) Will there be a difference of levels of guardianship based upon gender or race of the employee processing the transaction at each POS terminal?

Ho1: There will be an overall generalized absence of capable guardianship at the POS terminals during the face-to-face card in hand transaction, and the cashiers will not act as a capable guardians over the card accounts in keeping with Bank Rules, Visa and MasterCard

merchant agreement contracts in efforts to prevent identity theft. They will not take the card in hand at any point during the transaction to specifically compare the account number listed on the face of the card to that showing in the system nor will the cashier specifically check the back of the card to see if it has been validated by an authorized signature. Variable Hypotheses: 2) There will be a slight to significant difference between levels of guardianship when the purchase is an electronics purchase versus a non-electronic purchase or whether the purchase was made at the store's front end register or back electronic counter register. 3) There will be a higher level of capable guardianship demonstrated by participants at POS terminals when the charges to the credit card are over $50 versus those under $50. 4) There may be a slight difference in higher levels of guardianship depending upon the business of the store or lack thereof. 5) There will be no difference if the cashier is male nor female, Black or White. Overall, there will be a generalized absence of capable guardianship at the POS terminals within each store chain by all participants, with higher levels of guardianship being demonstrated only by those participants processing electronics purchases.

RQ2: Will the cashier at the face-to-face transaction at the POS (point-of-sale) terminal require the cardholder and purchaser to sign the back of the unsigned card used for purchase, and will he or she make her show a government issued photo identification for verification of her identity before the transaction is allowed to be processed through, in keeping with merchant agreement rules as mandated by Bank Rules and Regulations, Visa and MasterCard?

Ho2: The cashier will not check the back of the card, and therefore, will not check for an authorized signature validated the card. Consequently, the cashier will neither ask her to show a government issued photo identification document bearing her genuine signature for comparison or verifying her identity before the transaction will be allowed to be processed through to its

entirety. Ultimately, it is hypothesized that the cashier will not abide by the Bank Rules and Regulations, the Visa merchant rules for accepting unsigned cards, nor the MasterCard rules for accepting unsigned cards (See Appendices B, C, & D for references).

RQ3: Will the cashier act in lieu of an FDE (Forensic Document Examiner) to investigate by visual comparison the general similarities or differences of handwriting demonstrated on the government issued photo identification bearing a genuine signature of the researcher to that of the unsigned card that should be required to be signed in the presence of the cashier at the POS terminal?

Ho3: The cashier will not check the back of the card, and therefore, will not check for an authorized signature validating the card; thus, he or she will neither attempt to ask the researcher to sign the back of the card nor show government photo identification bearing her genuine signature, nor will he or she act in lieu of an FDE to investigate by general visual comparison the general similarities or differences of the handwriting on the government issued identification to that of the signature on the back of the card per requested signature. The cashier will not request a signature on the back of the card, and the only signature requested will be that prompted by the electronic signature capturing device at POS terminal.

RQ4: Will the cashier rely solely upon the electronic capturing device to verify the signature and not personally look at it himself or herself?

RQ5: Will the participant cashier at the POS terminal solely depend upon the EMC chip reader technology newly implemented at the POS terminals equipped with such to "guard" over the identity of the cardholder, even when neither a PIN number nor signature is required nor requested for the transaction to be processed?

Ho4 and Ho5: The cashier participant processing the transaction will demonstrate heavy reliance upon the electronic signature capturing device, if a signature is required, and/or the EMV chip reader technology to "guard" over the face-to-face card in hand sales transaction at the POS terminal, whether a PIN is requested or required or not.

Limitations of the Study

This field research was limited strictly to observations made as a credit card payment purchaser in 28 separate large department stores of three commonly targeted chains—all located within the tri-state region of Eastern Tennessee, Western Virginia, and Northeastern North Carolina and one in Georgia. Therefore, it lacks sufficient quantity for external validity and large generalizability. Additionally, it does not involve guardianship issues related to online identity theft and credit or debit card fraud that is also a major contributor of fraud. The internal validity is weakened in that this study only portrays the observations of those representatives sampled within this specific region. Therefore, the information gathered and coded for this analysis is restricted to observations only and not interviews with individual managers or employees, which may yield additional insight to findings. There is little criminological research done on this specific area of adequate guardianship at point of sale transactions involving in store merchant sales clerk employees or managers and their adherence to the merchant agreement contracts as mandated by Visa, MasterCard and Bank Rules (See Appendix B, C, & D). To date, no criminology research has been reported analyzing why large scale identity theft in credit and debit card fraud occurs at specific large department store chains or why they are strongly considered as suitable targets by motivated fraud offenders.

This field research study is the first of its kind and, therefore, limited to understanding the nature and origin of the problem from a criminological theoretical perspective and observations

made during first hand face-to-face transactions at POS terminals within three specific retail store chains only. Observing other retail store chains during card in hand transactions may yield different results depending upon the other merchant's rigidity of adherence to merchant agreement contracts and responsibilities of verifying identity of cardholders during POS face-to-face transactions. Other limitations also included are those inherently related to consumer profiling and these are restricted in this particular study to the investigator's personal characteristics and demographics of a white conservative middle-class middle-aged female. Consumers with various individual characteristics and demographics may prompt different reactions from the employees at POS terminals during face-to-face transactions yielding different results.

Definitions of Terms

For a clearer understanding of this thesis, the following terms are defined:

Authentication: "Authentication is the process of assuring that a credit card transaction has been initiated by an authorized user of that card. From the merchant's point of view, authentication means getting the right information from the consumer, and having it verified by the transaction network. In recent years, authentication has been stepped up by means including security codes on credit cards" (Creditcards.com/glossary, n.d.).

Authorization: "Authorization is an important concept for both credit cardholders and credit card merchant accounts. Every retailer has a purchase limit above which they must seek authorization from the card issuer before they can complete the sale. Such authorization can be done by telephone or electronically at the cash register. Authorization is used to control credit card fraud. Authorization is also the first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request

authorization for the sale. The acquirer then routes the request to the card-issuing bank, where it is authorized or denied, and the merchant is allowed to process the sale" (Creditcards.com/glossary, n.d.).

Authorized Transaction: "In credit card terminology, an authorized transaction is one that has been approved" (Creditcards.com/glossary, n.d.).

Bank Card: A bank card is a form of a plastic payment method that is distributed by one's bank and allows the account holder and thus, cardholder, to make purchases using one's card as either debit or credit payment while deducting available funds from one's account. All bank cards bear either the Visa or MasterCard logo and are subject to each one's respective rules and regulations for honoring the card at merchants' stores.

Capable Guardianship: Capable guardianship is one of the elements missing in the crime triangle developed by criminologists, Felson and Cohen (1979). The absence of capable guardianship is what contributes to crime occurrences. The presence of capable guardianship deters crime from happening. In the aspect of this thesis, capable guardianship in the environment of daily routine activities of shopping would require that the employees, specifically those at the POS terminals would vigilantly guard the sales transactions, checking for appropriate signatures and identity, in efforts to obey the rules and regulations set forth by Visa and MasterCard in their merchant agreement policies, to help prevent identity theft and card-present fraudulent transactions.

Cardholder: A cardholder is the person holding the card in hand in preparation of making purchases either online, or for this research purpose, in store during face-to-face transactions at POS terminals within each store. A cardholder has the responsibility of providing a genuine

signature and government issued photo identification for verification at POS terminals, when and if requested by the cashier or manager during transactions.

Card Present: "Card-present transactions are those in which a credit card is physically present. Merchants are charged different levels of fees by the card transaction processors (such as Visa, MasterCard), depending on the level of fraud risk. Card present transactions, because the card is available for inspection, are considered less risky and therefore carry lower fees than online or phone transactions" (Creditcards.com/glossary, n.d.).

Card Present Fraud: "Card-present fraud occurs when a credit or debit card is used to make an unauthorized transaction in a face-to-face setting, such as a grocery store checkout lane. This type of fraud may involve the use of the actual stolen card or a fraudulent duplicated card made using a card number and magnetic stripe information" (Creditcards.com/glossary, n.d.).

Card-Present (CP) Transactions: "Credit or debit card transactions conducted face-to-face, in which the card is physically swiped. Card-present transactions are considered more secure than card-not-present transactions, since a merchant can view the buyer, the card and the signature on it" (Creditcards.com/glossary, n.d.).

Chargeback: "A credit card chargeback occurs when a charge is reversed, returning credit to a credit card customer from a merchant. There are several parties involved, since a return transaction goes through the customer's bank, the credit card processing interchange (such as Visa or MasterCard) and the merchant's bank. Consumers can sometimes initiate a chargeback when they dispute a purchase made from a merchant" (Creditcards.com/glossary, n.d.).

Chip Enabled Terminal: "Point-of-sale terminals that have or are connected to a chip card reader, an EMV application and can process chip card transactions. ATMs can also be chip-enabled. (Creditcards.com/glossary, n.d.).

Chip and Pin Cards: "A type of 'smart card,' chip-and-PIN cards use computer chips to store and process information instead of, or in addition to, a magnetic stripe. A personal identification number (PIN) is required at point of sale. The technology has replaced older-style magnetic stripes in Europe and is being adopted in much of the world. The United States has been slow to adopt the technology, but has begun to do so, especially with credit cards intended for international travelers" (Creditcards.com/glossary, n.d.).

Chip and Signature: "Chip and signature describes a form of credit card authentication coming into use in the United States. Traditionally, American credit cards were authorized for use via the data on magnetic stripes on the backs of the cards. As their name implies, chip-and-signature cards have a chip embedded within them, and the authority to use them is verified by signature. Chip-and-signature cards are an advancement in security over magnetic stripes, but not as secure as chip-and-PIN cards, which are verified with a PIN number" (Creditcards.com/glossary, n.d.).

Cloning: "Cloning is a technique criminals use to make counterfeit credit cards with working, stolen credit card numbers. The credit card numbers are often obtained through skimming" (Creditcards.com/glossary, n.d.).

Credit Card: "A credit card is a payment card that is accepted by merchants, and which can be read at the point of sale. Credit cards offer revolving lines of credit to cardholders, which means they have the ability to pay balances over time" (Creditcards.com/glossary, n.d.).

Credit Card Number: "A credit card number is the unique number imprinted on a credit card. The first six digits on a credit card are called the issuer identification number. They identify the issuer -- Discover, or American Express, for example. The remaining digits of a credit card number are unique to the individual card. Credit card numbers are usually embossed, a remnant the days when a physical impression of credit cards were made through zip-zap machines" (Creditcards.com/glossary, n.d.).

Credit/Debit Card Fraud: Credit or debit card fraud is the act of stealing another person's identity for the purpose of using that person's account to purchase items for oneself or to be resold for profit. Credit/debit card fraud occurs when someone has used another person's plastic card payment method without permission and without being an authorized user on the account. Identity theft is the primary crime occurring, while theft is the secondary.

Crime Triangle: The "crime triangle" is a theory developed by criminologists, Marcus Felson and Lawrence Cohen, the creators of the Routine Activities Theory (1979). It demonstrates the convergence of three essential ingredients necessary for crime to take place—motivated offenders, suitable targets, and an absence of capable guardianship. See *Figure 1* below:

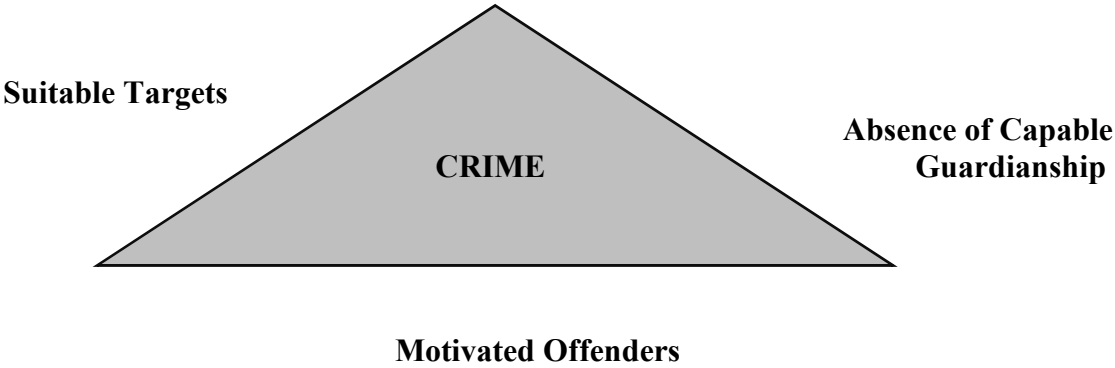


Figure 1. The "Crime Triangle" demonstrates the three necessary elements for a crime to occur: 1) Suitable Targets, 2) Motivated Offenders, 3) Absence of Capable Guardianship. This was developed by criminologists, Cohen and Felson (1979).

CVV: "CVV is one of the credit card industry's several acronyms for the credit card security code that helps verify the legitimacy of a credit card. Depending on the card, the security code can be a three-digit or four-digit number, printed on either on the back of the card or the front. CVV stands for 'card verification value' code. Other card issuers call their security codes CVV2 (Visa), CVC2 (MasterCard) or CID (American Express)" (Creditcards.com/glossary, n.d.).

Debit Card: "While debit cards and credit cards are alike in appearance, they differ in one critical aspect: A debit card withdraws money from a bank account, while a credit card creates a loan. Think of them as 'pay now' (debit) versus 'pay later' (credit). Today's debit card users often have the choice of authorizing transactions by either PIN or signature. While that choice often makes no difference to the consumer, it makes a great deal of difference to the merchant and transaction processors. A PIN transaction uses one payment system, the signature uses another, each carrying different fees" (Creditcards.com/glossary, n.d.).

EMV Card: "An EMV card, also called a chip-and-PIN card or smart card, contains a special computer chip to store card account data. Unlike magnetic-stripe cards, every time an

EMV card is used for payment, the chip creates a unique transaction code that cannot be reused, thus stymying counterfeit card fraud. The initials EMV stand for Europay, MasterCard and Visa -- the three processing firms that in 2002 first agreed to the standards. EMV cards are widespread in Europe and other parts of the world, and are being rolled out in the U.S."(Creditcards.com/glossary, n.d.).

EMV Chip Card Technology: "EMV® is a global standard for credit and debit payment cards based on chip card technology taking its name from the card schemes Europay, MasterCard, and Visa - the original card schemes that developed it. The standard covers the processing of credit and debit card payments using a card that contains a microprocessor chip" (*What Is EMV Chip Card Technology?,* n.d.).

EMV Liability Shift: "Under rules instituted by MasterCard, Visa, American Express and Discover, as of Oct. 1, 2015, in-store counterfeit fraud liability shifted to the party -- either the card issuing financial institution or the merchant -- that had not adopted EMV technology. Before, credit card issuers were primarily responsible for covering fraud affecting consumer accounts. While issuers will still reverse charges for fraud victims, they may now seek reimbursement from the merchant or merchant acquirer if the merchant had not installed EMV-compatible equipment when fraudulent charges were made on an EMV card" (Creditcards.com/glossary, n.d.).

Encryption: "In credit card terms, encryption is the process of encoding credit card information for secure transmission through credit card processing networks or across the Internet" (Creditcards.com/glossary, n.d.).

Face-to-Face Transaction: A face-to-face transaction is one that occurs inside the merchant's store and is processed via means of a card-present transaction, which is considered

by the credit card companies to be the least risky type since the employee has the opportunity to verify identity of the cardholder during the face-to-face transaction process.

False Positives: "In fraud detection, a "false positive" occurs when something innocent is wrongly deemed suspicious. Credit card holders encounter false positives most often occurs when a cardholder accidentally trips the card issuer's fraud detection system. Card issuers have developed sophisticated, automated fraud detection systems that work by detecting activities and patterns associated with fraud, but these systems don't work perfectly. False positives can cause a cardholder's transaction to be denied or an account locked down" (Creditcards.com/glossary, n.d.).

FDE: FDE stands for "Forensic Document Examiner" and is a professional that studies handwriting and can determine with expertise the differences between spurious signatures and handwriting and genuine signatures and handwriting for legal purposes. FDE's are often called upon in court to testify as to the validity of a document in question. For the purpose of this thesis research, the guardian at the POS terminal is called upon by the Visa and MasterCard regulations to fill the role of the FDE in store to visually compare the signatures on the back of the card to that of the government issued identification presumed to be bearing a genuine signature.

Fraud Alert: "A fraud alert is a security alert placed on a credit card account or credit bureau listing by either the customer or the issuer when a fraudulent account activity is either experienced or suspected" (Creditcards.com/glossary, n.d.).

Fraudulent Transaction: "A fraudulent transaction is one unauthorized by the credit card holder. Such transactions are categorized as lost, stolen, not received, issued on a fraudulent application, counterfeit, fraudulent processing of transactions, account takeover or other

fraudulent conditions as defined by the card company or the member company" (Creditcards.com/glossary, n.d.).

Fraudulent User: "A fraudulent user is an individual who is not the credit cardholder or designee and who uses a credit card account to obtain goods or services without the cardholder's consent. (Creditcards.com/glossary, n.d.).

Genuine Signature: A genuine signature is a signature that has been created by the person whose name the signature bears. It is a forensic document examination term that declares the true handwriting of the legitimate party involved. In this thesis, a genuine signature refers to the signature of the account cardholder on the back of the credit or debit card and verified by the genuine signature on the government issued photo identification.

Hacking: Hacking is the act of a person or persons involved in a crime ring who secretly gain access to a computer system in efforts to steal information. In this thesis, hacking can also refer to the actions of those who use skimming or shimming devices in order to gain access to legitimate account information of cardholders, for purposes of stealing the information to make fraudulent cards and purchase merchandise from retail stores illegally.

Identity Theft: "Identity theft, commonly shortened to ID theft, is generally defined as the use of personal information to commit fraud. The personal information used can vary; the more personal information a thief has, the greater the financial damage that can be caused. Identity theft can happen in many ways, through account hijacking, 'phishing,' dumpster diving or, sadly, by relatives stealing personal information" (Creditcards.com/glossary, n.d.).

Magnetic Stripe: "A stripe of magnetic information that is affixed to the back of a plastic credit or debit card. It can be black, brown or silver in color. It is the common type of card in the United States today. Often, it's called a 'magnetic swipe' card, because the card is activated by

swiping it through a device that can read the data in the stripe. The credit card's magnetic stripe contains three tracks of data. Each track is about one-tenth of an inch wide. The first and second tracks in the magnetic stripe are encoded with information about the cardholder's account, such as their credit card number, full name, the card's expiration date and the country code. Additional information can be stored in the third track. With the new generation of credit cards, such as chip cards, no magnetic stripe is needed. Also called magnetic strip or magstripe" (Creditcards.com/glossary, n.d.).

MasterCard card: "A card that bears the MasterCard symbol, enabling a MasterCard cardholder to obtain goods, services or cash from a MasterCard merchant or acquirer. (Creditcards.com/glossary, n.d.).

Merchant Agreement: "A merchant agreement is a document that lets merchants accept credit cards. It is a contract between a merchant and a bank and it lays out their respective rights, duties and warranties regarding how each will handle bank card activity" (Creditcards.com/glossary, n.d.).

Not Valid: A credit or debit card is considered "not valid" for purchases by Visa or MasterCard if it has not been properly and genuinely signed by the legal cardholder of the account on the back of the card within the signature strip. Near the strip reads the wording, "AUTHORIZED SIGNATURE – NOT VALID UNLESS SIGNED." If the card is not valid, rules and regulations require that the card must be signed in the presence of the cashier at the POS terminal and the customer must show proper government issued photo identification bearing the genuine signature of the cardholder for visual comparison.

Phishing: "Phishing is a criminal technique that uses computers to steal credit or debit card or bank account information. Consumers often see phishing attempts in the form of fake e-

mails that mimic those of banks. Consumers who click on such copycat e-mails will be transferred to a phony site that will try to dupe them into entering Social Security or bank account numbers" (Creditcards.com/glossary, n.d.).

PIN: "A PIN, or personal identification number, is a series of digits (usually four) used to verify the identity of the holder of a card. The PIN is a kind of password. Consumers often may choose whether to authorize a debit card transaction by signature or PIN; while it may make no difference to consumers, the choice means they are choosing different transaction processing systems" (Creditcards.com/glossary, n.d.).

POS: "The 'point of sale', or POS, is the location in a merchant's establishment at which the sale is consummated by payment for goods or services received. It is also where many retailers offer their store's credit card applications to consumers" (Creditcards.com/glossary, n.d.).

RAM scraping attack: "A process in which thieves hack a merchant's point-of-sale system and search its memory for payment card data while it is still being processed inside the terminal" (Creditcards.com/glossary, n.d.).

RAT: RAT or Routine Activities Theory is a criminology theory developed by two theorists, Marcus Felson and Lawrence Cohen (1979) that describes how crime must have three key elements in order to occur in our daily activities. These three elements are: 1) Suitable Targets, 2) Absence of Capable Guardianship, and 3) Motivated Offenders. (See *Figure 1*. Crime Triangle for reference.) According to Felson and Cohen, RAT can explain many crimes, particularly theft. By manipulating one of the elements of the crime triangle, crimes can be prevented. RAT is used to explain the theory behind this research thesis, and is demonstrated by the research itself in confirming the absence of the capable guardianship at the POS terminals

during face-to-face in store transactions with card in hand affording ample opportunities for back of card to be checked for proper signature and verified by proper identification, as mandated by Visa's and MasterCard's rules and regulations via merchant agreement contracts. Thus, if the absence of capable guardianship continues, the crime of identity theft and plastic card fraud continues; if the presence of capable guardianship replaces the absence, then the crime is deterred.

RFID: "Radio frequency identification (RFID) technology is increasingly used in everything from library books to key fobs that let office workers in their buildings to credit cards. They transmit very short range radio signals that a receiving device reads before it decides whether to let you check out a book, get to your cubicle or pay for that venti Cinnamon Dolce Frappuccino" (Creditcards.com/glossary, n.d.).

Security Code: "The security code on a credit card is the brief number that is printed on the card that helps verify its legitimacy. Depending on the card, the security code can be a three-digit or four-digit number, printed on either on the back of the card or the front, and goes by several names. The most common is CVV, which stands for 'card verification value' code. Other card issuers call their security codes CVV2 (Visa), CVC2 (MasterCard) or CID (American Express)" (Creditcards.com/glossary, n.d.).

Shimming: Shimming is an act of using a shimmer device, as those found last summer in Mexico at ATM machines, that sits between the EMV chip on the card and the chip reader to record the data on the chip as the card is being read by the ATM or POS terminal (Krebs, 2015).

Signature Strip: "A signature strip is an area on the back of a card coated with a white or gray material that holds ink. Imprinted above it are words to the effect of 'Authorized signature, Not valid unless signed.' Some people write 'Show ID' in place of their signature, in an effort to

discourage unauthorized use. While that may work in practice, merchants are not supposed to accept such cards" (Creditcards.com/glossary, n.d.).

Skimmer: "A credit card skimmer is a small device that lets a thief swipe a magnetic stripe credit card and surreptitiously record the information on it. A skimmer can be hand-held or installed where you would expect a legitimate card reader, such as an ATM machine or a gas pump" (Creditcards.com/glossary, n.d.).

Skimming: "Skimming is a method of stealing credit card information by using a small electronic device that scans and stores card data from the magnetic stripe. It can be done manually by a corrupt retail store employee who surreptitiously skims customers' cards, or by criminals who place a skimming device on top of a regular credit card reader (usually at gas stations or ATMs machines). Stolen credit card information can be used to make fraudulent purchases online or to clone new cards" (Creditcards.com/glossary, n.d.).

Smishing: "Smishing is a technique used by criminals to steal bank or credit card information using text messages. In such an incident, the mobile device user receives a fake text message that appears to be from a bank. The text message may request that the consumer call a phone number to provide card or account information to a criminal posing as a bank employee" (Creditcards.com/glossary, n.d.).

Spurious Signature: A spurious signature is a signature that is not genuine. The terminology relates to questionable signatures in the field of forensic document examination. In this thesis, it relates to the unsigned credit or debit card that would require a genuine signature, verified by identity documentation, in the presence of the capable guardian at the POS terminal, or failure to do so. If the cardholder and user provided a signature that was not able to be

visually comparable to that on a government issued photo ID, then it would be considered a "spurious signature."

Supercontrollers: For the purposes of this thesis, "Supercontrollers" are referred to as the employees (and managers training the employees, as well as merchants who are responsible for their employees). This definition expounds upon the idea set forth by theorists Sampson and Eck who argue "that not only should managers and employees act as guardians, but also act as "super controllers" (2010, p. 37). In their article, "Super controllers and crime prevention: a routine activity explanation of crime prevention success and failure," Sampson et al. raise awareness as to why people and organizations take (or fail to take) preventative action against crime (Bowers & Johnson, 2006; Knutson, 2006; Laycock, 2006 all as cited in Sampson & Eck, 2010, p. 37).

Synthetic Identity Theft: "Synthetic identity theft is when a fraudster creates a new and fictional identity from fake information or from combining some real identifying information with inaccurate or false information. Once crafted, the unreal synthetic identity is used to establish real bank accounts" (Creditcards.com/glossary, n.d.).

Terminal: For this thesis, a terminal is defined as the location of the register where the point-of-sale (POS) occurs. It is referred to throughout this body of text as the "POS terminal." This research accessed two specific terminal locations: 1) Electronics counters located in the back of individual retail stores used primarily for electronic purchases, and 2) Front registers located in the front end of each retail store used for general purchases, primarily non-electronic purchases. (See Table 3. *POS (Point-of-Sale Terminal Location within Store during Face-to-Face Transactions* for reference.)

Transaction: "(1) Any agreement between two or more parties that establishes a legal obligation. (2) The act of carrying out such an obligation. (3) All activities affecting a deposit

account that are performed at the request of the account holder. (4) All events that cause some change in the assets, liabilities or net worth of a business. (5) An action between a cardholder and a merchant or a cardholder and a member that results in activity on the cardholder account" (Creditcards.com/glossary, n.d.).

Two-factor Authentication: "Two-factor authentication is a form of identification often used in making sure a credit card transaction is authorized. Typically one factor may be a physical object (such as having a credit card in your possession), another may be a piece of knowledge (such as a PIN number or security code number), and yet another may be a unique characteristic (such as a fingerprint, an iris pattern or the ability to retype a sequence of numbers and letters). The presence of two factors allows a two-factor authentication" (Creditcards.com/glossary, n.d.).

Unsigned Card: An unsigned card is plastic card used for payment that the legal cardholder and account owner has failed to sign. Many people do not sign the back of their cards for fear of someone imitating their signature, but write "See ID" instead in the strip. This is still considered an unsigned card and does not validate the card for payment processing. The unsigned card is mandated by Visa and MasterCard rules and regulations to be signed in the presence of the cashier and verified by government issued photo identification bearing a genuine signature for general visual comparison purposes, before the transaction can legally occur. However, this practice has been and continues to be neglected in day to day practices at retail store POS terminals.

User Authentication: "User authentication is the process of validating a credit card user's identity or authorized user status. User authentication is an important part of a merchant's duties

in accepting credit card, although in practice, authentication has in recent years become often cursory or nonexistent" (Creditcards.com/glossary, n.d.).

Valid: For the purposes of this thesis, valid refers to the credit or debit card bearing a genuine signature by the legal cardholder, and account user, written in the signature strip on the back of the plastic card near the words, "Authorized signature, not valid unless signed."

Visa Card: "A card that bears the Visa symbol and which enables a Visa cardholder to obtain goods, services or cash from a Visa merchant or acquirer, and have the transaction processed through its network. Visa does not itself issue credit or debit cards, but partners with card-issuing financial institutions" (Creditcards.com/glossary, n.d.).

CHAPTER 2

LITERATURE REVIEW

Theory

How can one effectively and solely 'guard' one's bank accounts and credit card property sufficiently in a world rapidly and continuously advancing in technologies—even amongst the underground crime ring world? Despite the fact that laws have been enacted as guardians, and credit card companies continually add more security features to act as capable guardians, including the newest one of the EMV chip technology to institute safeguards, it is apparent that law, current security features and policy changes in and of themselves cannot entirely curtail identity theft and card fraud. There is still an overwhelming absence of capable guardianship. This phenomenon can best be explained by the routine activity theory (Cohen & Felson, 1979) that was first developed by criminologists Marcus Felson and Lawrence Cohen using a triangular model, which represents the convergence of three essential ingredients necessary for crime to take place—motivated offenders, suitable targets, and an absence of guardianship (see also: Felson, 1995; Felson 2002, 2006; Felson & Boba, 2010; Felson & Clarke, 1998). Bernburg and Thorlindsson (2001, pg. 546) report that several attempts have been made to study "routine activities with individuals as the unit of analysis" and these studies support the hypothesis that "deviant events are more likely to occur when routine activities, such as simply using one's credit card on a routine basis for purchases, increase the convergence" of time, space, absent guardianship at several different level, availability of suitable targets, and motivated offenders (Hawdon, 1996; Lasley, 1989; Massey et al., 1989; Miethe et al., 1987; Mustaine & Tewksbury, 1998a, 1988b, 1988c; Osgood et al., 1996; Sampson & Woolredge, 1987).

Ronald Clarke and Marcus Felson (1998) make an important transition from criminological studies of offenders to detailed analysis of criminal events and criminal activities

with their "crime triangle" (Lilly et al., 2011, p. 339). Together they explain the crime triangle based upon a rational choice perspective of offending as techniques of situational crime prevention. Routine activities theory was founded by Cohen and Felson (1979) describing how crime needs three essential ingredients to occur: motivated offenders, suitable targets, and an absence of capable guardians. Crime needs a convergence in space and time for all three to occur simultaneously. If one of the elements is missing, then crime cannot occur, according to the Cohen and Felson "crime triangle" model (1979). This means that a crime can be prevented by keeping motivated offenders away from suitable targets "at specific points in time and space" or "by increasing the presence of capable guardianship," (Kleemans et al., 2012, p. 87). By increasing efforts, increasing risks, reducing rewards, reducing provocation, and removing excuses valiant efforts can be made to prevent specific crimes that can occur during routine activities of everyday life (Kleemans et al*.,* 2012, p. 87-88). One particular area of crime that occurs in everyday life of American consumers, which is in great need of prevention and intervention by capable guardianship, is that of identity theft and credit/debit bank card fraud. This crime can best be explained theoretically by routine activities theory (Cohen & Felson, 1979). Routine activities theory has been applied by various criminology researchers in efforts to explain a variety of crime issues for more than 30 years (Boetig, 2006, p. 12). These include robbery, rape, residential burglary and theft (Boetig, 2006, p. 13-14). This paper will extend the application of routine activities theory from physical thefts to include stealing from remote locations as will be described in methods of identity theft and credit card fraud. Applying the routine activities theory approach, this thesis has attempted to explain how this phenomenon's various aspects are completely understood by using this criminological theoretical structure. Understanding this theory is critical to investigating and understanding credit card fraud.

Credit Card Fraud

For many years now, it has been a known fact that credit card fraud has become a growing problem not only within the United States, but also within the international global economic community. According to the latest statistics published by the U.S. Department of Justice in their recent publication of *Victims of Identity Theft*, *2014* alone an "estimated 17.6 million persons, or 7% of all U.S. residents age 16 or older, were victims of one or more incidents of identity theft," up from the 16.6 million persons reported in 2012 (Harrell, 2015). Surprisingly, two-thirds of these suffered direct financial loss of $99 or less that involved fraudulent plastic card purchases. Accumulatively, "direct and indirect losses from identity theft totaled $24.7 billion in 2012" (Harrell, 2013). There is an estimated minimum loss of 800 billion English pounds per year due to credit and debit card fraud worldwide (Gee et al., 2010 as cited in Papadopoulos and Brooks, 2011, p. 222). Interestingly enough, 71% of all worldwide revolving credit cards in operation today were issued in the US, according to FBI Special Agent Slotter, who served as a CPA in the New Haven, Connecticut Field Office (Slotter, 1997, p. 2). In the United States alone, Visa and MasterCard reported a loss of $875 million US dollars in 1995 (Slotter, 1997, p. 2). With credit and debit cards rapidly replacing cash and check transactions for many businesses, new opportunities are presented daily for exploitation. The American Bankers Association reported that 45% of US consumers used less cash and more plastic payment methods between the years of 2004 and 2006 (Smith, 2007, p. 37). Consumerism is a cultural way of life in America, but it appears using cash for transactions are becoming less of a tradition. As many gluttonous American consumers, having insatiable appetites (Durkheim, 1951) are attempting to maintain popular consumerist lifestyles, people of this country are extremely vulnerable. Oftentimes, many have easily fallen prey to victimization by others in

deviant acts of fraud unknowingly. As legitimate credit or bank debit card owners, people are advised to diligently and vigilantly protect their personal identifying information and property from identity thieves and potential credit/debit card fraudsters, and to check their accounts regularly. Educational efforts are made by the CIA in distribution of brochures for bank customers intended to teach one how to maintain financial security and prevent identity theft resulting in potentially costly damages and fraudulent purchases to an owners' accounts. This education has helped raise awareness and consciousness about the prevailing issue of identity theft and card fraud. More recently, a number of news reports have aired raising awareness to the public as well. However, in today's technologically advanced global society of economics—readily accessible to the criminal—it appears this type of self-guardianship is not sufficiently adequate, leaving a tremendous deficit of capable guardianship of one's own identity, as well as one's own financial information and security.

Intertwined Problem of Identity Theft

The severity of credit card fraud cannot be properly understood without first having a thorough understanding of identity theft. Identity theft, which acts a predecessor to plastic card fraud, has quickly become "the most prevalent financial crime in the United States" (White & Fisher, 2008, p. 3). Identity theft can occur on various levels including individual offenders, co-offenders, and organized crime group offenders. Identity theft can be defined as the unlawful use of another's personal identifying information whether it be name, address, social security number, government passport number, driver's license number, biometric information, bank account or credit card account information in attempt to gain access to services or finances with criminal intent (Allison et al*.,* 2005, p. 19). Various criminologists propose different theories to explain the crime of identity theft, which will be discussed in the following section. Professor

Robert Clarke (1994) developed the current theory of human identification to explain the crime of identity theft and defined it as "the association of data with a particular human being" (LoPucki, 2001, p. 95). Clarke (1994) applies his definition of human identification theory as a comprehensive overview of why humans choose to use another persons' data to identify themselves. However, other researchers have explained it in different ways. The following section will describe criminology theories that others have used to explain the convoluted crimes of identity theft and financial fraud:

Empirical Studies and Research Theories Explaining Identity Theft

Relatively, little empirical research has been done on "the prevalence of the crime, its clearance rate by arrest, or the demographic characteristics of the victims and the identifiable offenders," but criminologists from the University of South Florida and University of Illinois at Chicago reported that the typical apprehended offender was "African American, female, unemployed, working alone, and was unknown to the victims," who tended to be White males (Allison et al., 2005, p. 19). An important attempt to explain this type of individual offence with a routine activities approach is the study of Osgood et al. (1996), which argues that the motivation to deviate emerges from situations where the deviance is "symbolically and tangibly rewarding" (Osgood et al.,1996 as cited in Bernburg & Thorlindsson, 2001, p. 547). Applying this theoretical expansion to explain these typical identity theft offenders in a society that is wrecked with racist hate crimes and White male supremacy, it is not difficult to understand how a Black female could become motivated to choose a White male victim as a suitable target for offense. After all, it is the White males of the American society that represent the majority of politicians, police and judges who send disproportionate amounts of African American males to prison, leaving behind many Black females to financially support their children in the absent

fathers' places. By attacking White males as suitable targets, the African American females are not only finding revenge by robbing these men of their identities, but also doing so in a very "symbolic and rewarding" way—both psychologically and financially.

Two other researchers, Heith Copes and Lynne Veiraitis, from the University of Alabama at Birmingham and the University of Texas at Dallas respectively, jointly conducted two separate studies on the bounded rationality of identity thieves and the use of the neutralization theory for interrogations of identity thieves (Copes & Veiraitis, 2009; Copes, Veiraitis, & Jochum, 2007). The first of their two studies was conducted in 2007 using the techniques of neutralization theory, which lists five specific techniques: (1) denial of responsibility, (2) denial of injury, (3) denial of the victim, (4) condemnation of the condemners, and (5) appeal to higher loyalties (Sykes & Matza, 1957 as cited in Lilly et al., 2011, p. 103). Using data from 59 federally convicted identity thieves, they provide illustrations of how information can be used to "develop functional themes" for police Reid interrogation procedures. Their study attempts to bridge the gap between theory and application by helping the police interviewers understand the mindset of the identity thieves and justifications used by them both prior to the crime and after the event in efforts of obtaining confessions by guilty suspects. Their sample included offenders from ages 23 to 60 years old, with 18 White females, 16 African American females, 2 Asian females, 8 White males, and 15 African American males (Copes et al., 2007, p. 452). Again, there is a dominant pattern of African Americans, both male and female, disproportionately represented to Whites, in this sample of convicts. Overall, 35 of these offenders used a minimum of one neutralization technique while 14 used multiple techniques. The most frequent techniques that these identity thieves mentioned were: "denial of injury (n=21), appeal to higher loyalties (n=14), denial of victim (n=9), and denial of responsibility (n=6)" (Copes et al., 2007, p.452).

One of the most common statements made by the offenders was "I always thought that just because it was a white collar crime it didn't hurt nobody," as they tried to deny causing any real harm from stealing a person's identity and credit, while justifying themselves and neutralizing the act itself (Copes et al., 2007, p.452). Others brazenly stated that "Everything that I did was based on grabbing the identity and then opening separate accounts. It affected them, but it was different," (Copes et al., 2007, p. 453). Different in what way, others might ask? Researchers soon discovered that inside these identity thieves' criminal minds, it was easy to justify victimizing a faceless, plastic card. Identity thieves argue that the "only people that actually lose from their crimes are banks, corporations, and other deserving victims," (Copes et al., 2007, p. 453). The identity thieves claim it is only a minor hassle to the victims, and unauthorized charges can be easily dropped with a few phone calls, warranting reimbursement by the bank to the victim (Copes et al., 2007, p. 453). As one anonymous offender said it:

> Intentionally screw someone over…I couldn't do it... but corporations, banks, police departments, government—oh, yeah, let's go get 'em. Because that's the way they treat you, you know what I'm saying. If they done screwed me over, screw them. (as cited in Copes et al., 2007, p. 453)

Little do these offenders realize that the costs of their crimes are passed from the banks and corporations to the customers in forms of higher prices, higher interest rates and taxpayer funded government bailout assistance programs for re-imbursements. As a result, all people bear the costs, including the offenders as consumers and taxpayers. Another offender claimed:

> I did it for my son. I thought if I had money and I was able to live, have a nice place to live, and not have to worry about a car payment, I could just start a new life and that life is for him. (as cited in Copes et al., 2007, p. 453)

This statement could likely have been made by one of the African American females in the group of offenders, who as previously described in Allison et al.'s 2005 study, targeted White males to steal identity in vengeance, as she faced the financial crisis of raising her child alone as a struggling single parent, in the absence of his father in prison. For single parents, it is easy to comprehend that desperate times can call for desperate measures, and caring mothers will do almost anything to provide for their child. However, if a mother takes irrational risks by committing crime and landing herself in prison, it shows very poor rationale: The child is now left alone suffering two absent parents, instead of only one absent father. This concept of rationale leads to the next study of bounded rationality of identity thieves.

In 2009 Copes and Vieraitis explored how offenders' experiences affected their rational assessments of risks versus rewards in a cost benefit analysis, which in turn facilitated their decision to engage in identity theft as an easy, rewarding and a "relatively risk-free way" of funding their lifestyles (Copes & Vieraitis, 2009, pg. 237). By gaining the offenders' perspectives and analyzing them through a theoretical rational choice framework (Cornish & Clarke, 1986), researchers were able to understand what factors influenced their criminal motivations (see also Clarke & Cornish, 2001). Rational choice theory, fitting hand in hand with routine activities theory (Cohen & Felson, 1979), and provides solid infrastructural framework to support the leg of the triangle that represents the motivated offender. Copes and Vieraitis discuss the various laws which have been enacted since the 1990s, including the Identity Theft Assumption and Deterrence Act (1998), the Identity Theft Penalty Enhancement Act (2004), the Fair and Accurate Credit Transactions Act known as FACTA (2003), as well as the National Fraud Alert system—an offspring creation of FACTA. According to these researchers' perspective, all of the laws mentioned above have been applications of routine activities theory:

> Most current legislation is directed toward creating or strengthening existing consumer protection laws and is based upon the assumption that potential offenders will be deterred by increased guardianship over targets or the threat of steeper penalties if caught. (Cope & Vieraitis, 2009, p.241)

In the same vein of routine activities and rational choice theories, their research revealed the primary and suspected motivation for offenders instigating identity theft was, of course, the desire for money (Cope & Vieraitis, 2009, p. 245). As one offender put it, "It's all about the money. If there ain't no money, it don't make no sense" (as cited in Cope & Vieraitis, 2009, p. 245). Therefore, money is the driving force behind most economic crimes, including identity theft and credit card fraud. For many of the offenders, the research interviews revealed that identity theft was an easy way of getting quick cash and "getting high" for those centered on self-indulgence (Cope & Vieraitis, 2009, p. 246). Other rational choice presented by the offenders was that of making profitable use of their employee positions of guardians over another person's sensitive personal and account information either misusing it themselves or selling it to others illegally for profit. They conclude their study with principles of situational crime prevention methods that could send deterrence messages at the point of sale, or scene of the crime by reducing the attractiveness of the suitable target. Also, they discuss promotional support of public campaigns designed to create an impression that law-enforcement agencies consider identity theft, and therefore credit card fraud, a serious crime that promises to be prosecuted to the fullest extent (Copes & Vieraitis, 2009, p. 250-258). This study strongly supports the idea of deterrence based situational crime prevention with convergence of space and time, motivated offenders, suitable targets and lack of guardianship as identified by routine activities theory.

Other more recent studies by Australian researchers from the School of Business at Queen's University and University of New South Wales, report contrasting findings to those discussed above (Free & Murphy, 2014, p.1-41). In their personal interviews and study of 37 convicted felons of fraud related to identity theft, results showed that many of these types of crimes are not predicated upon solo-offending, but rather on co-offending (Free & Murphy, 2014, p. 1-41). This co-offending pattern can also be explained by routine activities theory in the social context by "opportunities that arise in everyday life," emphasizing that the socio-structural patterns of people's routine activities can bring together, or converge, motivated offenders—rather than just one single offender—with suitable targets lacking capable guardians (Bernburg & Thorlindson, 2001, p. 543-560). While Cohen's and Felson's (1979) routine activities theory is applied to explain co-offending in this social context, others could explain co-offending by applying Sutherland's (1949) differential association theory. Differential association relates one's opportunity to commit crime to whom one regular associates with socially, and by whom cultural transmission is attributed. This theory explains the opportunity of gaining access and knowledge of 'how' to commit a specific crime, such as identity theft and credit card fraud.

Whether it be differential association theory (Sutherland, 1949), techniques of neutralization (Sykes & Matza, 1972), low self-control (Gottfredson & Hirschi, 1990), or rational choice theory (Cornish & Clarke, 1986), it is obvious that mainstream criminology has tended to focus on the offenders rather than the criminal events and criminal activities themselves, as can be understood and appreciated by the research described above. However, Cohen and Felson (1979) take a different approach by not necessarily trying to discover the special characteristics of offenders, but rather the identifying circumstances that facilitate the criminal event. This approach makes prevention of crime potentially more implementable. It is this approach that

also explains a wide array of crime architectures, including organized crime rings, which have been found to commit massive amounts of identity thefts and credit/debit card fraud (Baldwin, 2002, p. 8).

According to Netherland law researchers, Edward Kleemans, Melvin Soudijn, and Anton Weenink, organized crime research shows that some offenders have quite normal characteristics as individuals—although, they are involved in serious crimes. These researchers concur with the routine activities approach to solving organized crime. In an article entitled, "Organized crime, situational crime prevention and routine activity theory," seven papers "in which ideas on situational crime prevention and routine activity theory are applied to issues of organized crime and terrorism," (Kleemans et al., 2012, p. 89). All the papers were prepared by researchers for the Dutch National Police Agency and were presented during a meeting with Ron Clarke of *Trends in Organized Crime* (Kleemans et al., 2012, p. 89). Each paper's special topic discussed various types of organized crime applying the routine activity approach. One paper revealed how willing offenders can and do outwit capable guardians (Huisman & Jansen, 2012, as cited in Kleemans et al., 2012, p. 89). It also discussed the convergence of trailer park settings, making the group characteristics of social bonds, reputation and culture of silence all instrumental in creating a void where there is no capable guardian. The void was protected by psychological barriers further preventing any effective guardianship from developing. It is within this same context, yet different environment that organized Asian, Latino and African organized crime rings of identity thieves and credit card fraudsters maintain their void of capable guardians.

Soudijn and Zegers focused their paper on another issue that is highly relative to organized identity theft and credit card fraud. Their research paper discussed how cybercrime and virtual offenders, who commit fraud online, converge in physical settings such as local tough bars to share information as mutual offenders of the same organizational crime ring. By

reviewing 150,000 posting by 1,846 members, researchers discovered that "hacking accounts and stealing money is not their biggest problem: the main risk is not leaving traces when wiring the money into other accounts," (Soudijn & Zegers as cited in Kleemans et al., 2012, p. 90). The virtual world of internet organized crime rings makes the concept of space much different than the physical world. It offers much more barriers and darkness from exposure, while creating the ultimate void of capable guardianship. It also allows offenders from different parts of the world to 'meet,' 'rate each other,' and continue business bilaterally, while they remain completely shielded from the authorities; in this way, they are able to find suitable co-offenders (Soudijn & Zegers as cited in Kleemans et al., 2012, p. 90). Finding suitable co-offenders has a snowballing effect creating large organized crime rings that have a tremendously damaging effect on stealing identities in mass quantities, as well as stealing money from numerous accounts in exorbitant amounts. Here is an excellent example of how routine activities theory is applied to explain the extreme absence of capable guardianship online from hackers who steal identity and credit card information. Hence, the papers presenting these special organized crime issues underline the necessity to move beyond the traditional 'crime triangle' of motivated offenders, suitable targets, and the absence of capable guardians, and expand this theory conducting further empirical research (Felson & Clarke, 2012, as cited in Kleemans et al., 2012, p.91).

Effects of Identity Theft on Card Users

Although identity theft consists of three different types: financial, nonfinancial, and criminal record—financial identity theft accounts for the largest portion of these three and warrants great concern for implementing capable guardianship—with losses continually rising from the $2.3 billion estimate reported by the U.S. General Accounting Office in 2002 (Allison et al., 2005, p. 19). In 2003 alone, more than 10 million cases were reported (Gerard, Hillison, & Pacini, 2004

as cited in White & Fisher, 2008, p. 3). Within the previous 5 years prior to this report, 27 million Americans reportedly had been victims of identity theft (White & Fisher, 2008, p. 3). Methods used to commit identity theft range from low-tech methods to high-tech methods and include thefts of wallets, purses, dumpster diving, hacking into databases and personal accounts online using viruses or decoding techniques, and more prominently by using specialized equipment (Barker et al., 2008, p. 402-404; White & Fisher, 2008, p.3). In computer-related identity theft, the offender may be in another part of the state, country or the world (White & Fisher, 2008, p. 8-15). This is a perfect example of how an absence of capable guardianship over various people located in different parts of the world, but functioning within an online cyber world and targeting victims to fraud from other remote locations of the globe, creates massive opportunities for identity theft and credit card fraud online. This is all accredited to the absence of capable guardianship concept of routine activities theory. This will be discussed further in a subsequent section. Hence, most methods of identity theft are not amenable to police suppression efforts, which condition further exacerbates and demonstrates an absence of formal guardianship and legal protection over an individual's identifying account information before becoming victimized (White & Fisher, 2008, p.4). Laws enacted, that have been previously mentioned, deal primarily with deterrence and aftermath of fraud, and only yield mild preventions of true security and protection from attack. Devices, such as skimmers, are used for stealing legitimate credit card information. Additionally, there is equipment for making counterfeit credit cards, which is readily available to anyone who wishes to make a small investment to beat the system (Barker et al., 2008, p. 400-401). The prices range between $300-$500 for skimmer devices and $5,000-$10,000 for equipment to manufacture fake credit cards (Barker et al., 2008, p. 401). Unfortunately, "there have not been any laws or legislation put in place against the skimming and counterfeit card devices," (Merchant Account Blog 2006 as cited

in Barker et al., 2008, p. 403). More recently, since the new EMV chip technology has been encrypted into cards, there has been the underground development and sale of "shimmers," which are capable of reading EMV chips.

The Challenge of Capable Guardianship

The question posed to the reader: How can one effectively and solely 'guard' bank accounts and credit card property sufficiently any longer in a world rapidly and continuously advancing in technologies? Although laws, policies and new security features, including the EMV chip technology, have been enacted to act as guardians, is it feasibly possible? It is strongly suggested that none of these precautions can entirely stop identity theft and card fraud, nor effectively deter and curtail it significantly. There yet remains an overwhelming absence of capable guardianship—and surprisingly at in-store POS terminals during card in hand face to face transactions with merchant employees—places believed to be the least risky sales venue by most credit card companies. This phenomenon can best be explained by routine activity theory (Cohen & Felson, 1979) which was first developed by criminologists Marcus Felson and Lawrence Cohen using a triangular model, which represents the convergence of three essential ingredients necessary for crime to take place—motivated offenders, suitable targets, and an absence of guardianship (see also: Felson, 1995, 2002, 2006; Felson & Boba, 2010; Felson & Clarke, 1998). Bernburg and Thorlindsson (2001, p. 544-549) report that several attempts have been made to study "routine activities with individuals as the unit of analysis" and these studies support the hypothesis that deviant events are more likely to occur when routine activities, such as simply using one's credit card on a routine basis for purchases, increase the convergence of time, space, absent guardianship, availability of suitable targets, and motivated offenders

Hewson, 1996; Lasley, 1989; Massey et al., 1989; Miethe et al., 1987; Mustaine & Tewksbury, 1998a, 1988b, 1988c; Osgood et al., 1996; Sampson & Woolredge, 1987).

In the absence of sufficient guardianship needed to protect one's identifying information, counterfeiting cards are going to continue to become a growing problem according to Katherine Barker, Jackie D'Amato and Paul Sheridon—researchers at the College of Business, University of South Florida (Barker et al., 2008, p. 406). Since the effect of fraud costs not only the victims, but also the entire system of banks, merchants and credit card companies, various fraud programs have been implemented for deterrence and detection by the same. The guardianship efforts have expanded from the sole responsibility of the individual and shifted to a broader system of government through laws, and businesses through protective designs. Visa, American Express and MasterCard have developed and added more elaborate physical features to legitimize credit cards. These features have in the past included holograms, fine-line printing, and ultra-violet pink to reveal the credit card company's logo under special lighting, thus making duplication more difficult—but not impossible. Additionally, programs geared toward verifying legitimate card ownership were launched by implementing CVV codes within the magnetic strips of the cards. When the card is used at the point of sale, an encrypted CVV code is read by the POS terminal and transmitted to the issuing bank where the code is verified. This method is also an attempt to provide more adequate guardianship over the account, and was designed to protect users' personal identifying and credit/bank card information. Howbeit the method has not succeeded in eliminating fraud. Much to everyone's dismay, these guardianship efforts promulgated by credit card companies offered only small victories. Cardholders were ever-increasingly inundated and trumped by fraudsters with the aforementioned skimming devices, which can read the magnetic strip, as well as the CVV code on the back of the card, and capture all the necessary verifiable information (Barker et al., 2008, p. 404). The newest EMV chip

technology in the process of implementation within the United States is carrying great expectations that it will tremendously help in curtailing the crimes of identity theft and card fraud. However, many registers at stores are not equipped to handle these transactions yet, despite the liability shift that took place, October 1, 2015. The EMV model taken from the European chip encrypted cards in Europe and the United Kingdom requires both the chip and a PIN number to be used for purchases. However, this is not the case within the U.S. where even those companies that have transitioned over to the chip reader do not yet regularly require a PIN number for the card transaction to be completed as is demonstrated by this research in subsequent chapters. That said, even PIN numbers assigned specifically to individual cardholders are able to be easily stolen, and this paper will soon reveal how. The overall picture is that there continues to be a great absence of capable guardianship, and the word to focus on here is "capable."

For instance, a capable guardian in a retail store setting is one that takes all necessary precautions and steps as outlined by the merchant contract agreement and guidelines of properly checking for an authorized signature on the back of each consumer's card during face to face card in hand transactions. He or she also requires that the consumer sign the card in his or her presence if the card is blank and unsigned. Subsequently the capable guardian will follow up with requesting government issued photo identification bearing a genuine signature and will then make general visual comparisons for similarities or differences between the two signatures. Additionally, he or she will be actively engaged and aware of suspicious consumer behaviors, such as those outlined by Visa in their "Card Acceptance Guidelines for Visa Merchants" (2015, p. 35). Europe nor the United Kingdom massively utilizes the electronic signature capturing devices that the United States uses for signatures for in store POS transactions, so there is not a reliance upon these devices for security measures as there is in the United States. Most

merchants and employees largely use the old fashioned way of each individual employee visually comparing each handwritten signature of each card purchaser during each transaction and requiring government issued photo identification—and they do so somewhat consistently no matter what the specific business establishment genre. This was discovered by this researcher during travels for an independent study within England and France in the months of May-June, 2014.

The Places a Consumer is at Risk

Based upon the routine activities theory and this principle precedence of the absence of capable guardianship, efforts have been made by online businesses to warn consumerist cardholders. Special warning is giving to those who have false sense of security and feel safer using their bank debit card versus their credit card for transactions. Educating the consumer about the places which pose the greatest risk and why, Bankrate.com discourages using one's bank debit card at four specific places known for victimization (http://www.bankrate.com). These four places include large department store chains, outdoor ATMs and outdoor pay-at-the-pump gas terminals, restaurants, and the World Wide Web (http://www.bankrate.com). The reasoning behind this rationale is that most of these places lack appropriate guardianship, thus making them a great suitable target for motivated offenders. Fraudsters can slip around in the dark to these hot spots for crime, place skimming devices over the real card slots at ATMs and other terminals such as these, and steal a mega amount of information in a short time. This makes one's risk for identity theft and credit card fraud extremely high (http://www.bankrate.com). "If the public has access to it, then someone has the ability to add skimming devices to it, position cameras on it and position themselves in a way where they can surveil it," (Bell, 2014 as cited online at http://www.bankrate.com).

Outdoor terminals. For instance, someone can sit from inside a car across the street with their laptop and antenna receiving and downloading all the pertinent information needed for debiting and draining one's account before the victim ever makes it home. By using small cameras to capture footage of debit card users, while they are entering their personal identification number, or PIN, the fraudster is gaining free access to the victim's money (http://www.bankrate.com). He or she inherently triumphs over the rightful guardianship and authority of the cardholder and bank, while wrongfully assuming the guardianship role of the account themselves by interception. Victimization of both the bank and the unaware card holder occurs as a result. This describes one of the many ways that cardholders can become victims of credit/debit card fraud while still holding their card in hand. All outdoor credit/debit card terminals make the legitimate cardholder an open target and unknowingly leave them vulnerable to attack. According to this website, one is much better off using terminals inside retail outlets or other high-trafficked, well-lit places (Bell, 2014 as cited online at http://www.bankrate.com). These places offer guardianship in the way of plenteous customers passing by, and by dispelling darkness so that a fraudster is less capable of hiding himself and his equipment. As one moves through each phase of identity theft and credit/bank card fraud, one can better realize and appreciate the routine activities theoretical underpinning, which best explains this phenomenon and how the necessary guardianship concept continues to be problematic (Cohen & Felson, 1979).

Restaurants. Another dangerously risky place to use one's bank debit cards it at restaurants. This is due specifically to the lack of capable guardianship over one's card when it is being processed. It is common procedure for wait staff to take one's card, usually nestled within a black vinyl pouch with one's bill, away from the table and therefore away from the

oversight and guardianship of the owner of the card. Once out of sight, the card can be secretly skimmed on equipment and the entire customer's credit information is therefore saved for identity theft and financial fraud. If one is paying with a bank debit card versus a credit card, this can be even more risky because the wait staff/fraudster can drain the account in one lump sum before the customer ever leaves the building. Due to the high frequency of this phenomenon, some restaurant owners have invested in newer equipment that allows the wait staff to process the plastic card payment directly at the table and completely in the view of the customer card owner. This whole concept is based strictly upon the routine activities theory, allowing the customer to maintain capable guardianship over their card and account by keeping the transactions out in the open and not behind closed doors somewhere else in the restaurant. It is apparent in this illustration that the absence of capable guardianship, converging with the opportunity in time and space giving direct access to the customer's card, allows motivated (and usually low wage earning waitresses/waiters) ample access and opportunity to commit crimes of credit/debit card fraud. "Would you care for a side of credit or debit card fraud with your meal?" is a question that wait staff does not ask the customer, but probably should. In an interview, McGoey stated that any place where the credit card is out of hand can increase chances of fraud: "The guy comes to your table, takes your card and disappears for a while, so he or she has privacy"....giving the person plenty of time to copy your card information (http://www.bankrate.com).

Online. Another illustration of how routine activities theory is effectively applied to explain identity theft and credit/debit card fraud is the relationship between the online cyber world of e-commerce and the potentially damaging effects of hacking, due to absence of capable guardianship. Online is the number one place that people should not use their credit or debit

cards, according to the previous source cited. There are multiple ways that data can be intercepted and compromised by invasive malware software of hackers, without the knowledge of the consumer—until long after the damage is done. According to Hendi Yogi Prabowo, researcher for the Centre for Forensic Accounting Studies at Islamic University of Indonesia, "credit card fraud has become one of the most sophisticated crimes of the world" and that "global payments fraud statistics suggest that more must be done to address the problem" (Prabowo, 2011, p. 371). Prabowo compiled studies using primary and secondary data from payment systems of the "USA, the UK, Australia and Indonesia to conduct historical and benchmarking analyses to highlight the trends in credit card fraud prevention in four countries," (Prabowo, 2011, p. 371). He explained these overall phenomena with the "crime triangle" of routine activity theory describing the three factors that allow crime to occur: motivated offenders, suitable target and absence of capable guardianship (Prabowo, 2011, p. 371).

In his article entitled "Building our defense against credit card fraud: a strategic view," he references Clarke's proposal that growth and technology has created new crime opportunities (Clarke, 2004, p. 55 as cited in Prabowo, 2011, p. 372). Using routine activity theory (Cohen & Felson, 1979) the author describes how another criminology theorist, Yar (2005), suggests that online crime expands the terrestrial concept of suitable targets to a whole new complexity that is significantly different in "value, inertia, visibility, and accessibility" measuring it with a concept called VIVA (Yar, 2005, . 424 as cited in Prabowo, 2011, p. 372). Of these suitable targets for online crime, those include the card not present ones. With a changing environment for remote purchases and cashless society, electronic commerce is replacing an immense number of real world transactions with virtual world purchases. Other theorists, Newman and Clarke (2002), propose that these motivated online offenders are driven by "criminogenic attributes of

information systems" known as SCAREM (as cited in Prabowo, 2011, p. 372). SCAREM is an acronym that stands for stealth, challenge, anonymity, reconnaissance, escape and multiplicity. Newman and Clarke propose that the offenders have overwhelming desire to beat the system, being sneaky and secretive and find that online environment offering great anonymity and thus "deception is everywhere" [online] (as cited in Prabowo, 2011, p. 373). Escaping the scene of the crime is easy for the online offender and avoiding detection ("reconnaissance"). This ease allows for quick and easy multiplication of the offences.

> For example, when a hacker managers to steal a bank's customer account information he may then use such information to facilitate the commission of other crimes such as extorting money from the bank for the return of the database. (Newman & Clarke, 2002; Newman & McNally, 2005, p. 42, as cited in Prabowa, 2011, p. 37)

New crimes emerge from the original crimes of stealing identities and credit/debit bank card accounts and they are all supported by the crime triangle of the routine activities theory (Cohen & Felson, 1979). The absence of capable guardianship, along with virtual world suitable targets, makes for a fertile environment for breeding online bank account crimes. The online world is now a predominant crime scene for convergence of the victim and offender, yet not in space, but within a network of the internet systems or perhaps the mail/package delivery system. Reyns (2010, p. 58) further explains how the motivated offenders and suitable targets do not have to even converge online at the same time, but can be at different times (as cited in Prabowo, 2011, p. 373). This expands routine activities theory even further eliminating the element of simultaneous 'time' in order for crime to occur.

In addition to this, the online environment creates great challenges for law enforcement to effectively establish guardianship. According to some criminology theorists, the success of guardianship depends primarily on the guardian's co-presence with the potential target and the potential offender at the same time and place (Yar 2005, p. 423 as cited in Prabowo, 2011, p. 373; Tseloni et al., 2004, p. 74). Yar argues that in relation to cybercrime maintaining a social or physical co-presence is ultimately almost impossible because the offender is highly mobile and his or her online activities are temporary and irregular, and thus warrants a need for adaption of the concepts and practices of guardianship to cope with the new environment (as cited in Prabowo, 2011, p. 373). Using certain analytic programs, some applications of industrial strength analytics have been employed across a wide variety of activities by certain credit card companies and banks in attempts to detect, or police, online financial fraud. Authors Bolton and Hand of the Institute of Mathematical Studies offered a comprehensive review of how technological advances using mathematical methodologies can be used to detect fraud once prevention, or presence of capable guardianship, has failed (Bolton & Hand, 2002, p. 235). In addition to this statistical fraud detection defense tactic, the US, the President's Identity Theft Task Force (2007) issued a strategic plan in April 2007 to tackle the surmounting problem of identity theft and financial frauds in America. Other countries have been attempting to coordinate efforts also (Prabowo, 2011, p. 381). Efforts to effectively protect and guard people from identity theft and credit/debit bank card fraud has been underway for more than a decade, yet the absence of truly capable guardianship causes this online environment for fraud crimes to prevail. Online fraud victimization has been contributed to low self-control theory (Gottfredson & Hirschi, 1990), since some levels of cooperation is often needed between the victim and the offender with the promise of goods, services or other benefits that may be nonexistent or that the

fraudster never intends to provide (Holtfretter, Reisig & Pratt, 2008, p. 190). Other studies exploring the idea of computer crime victimization using other theories including routine activities theory: Choi's integrated theories and empirical assessments reported in the January-June 2008 issue of *International Journal of Cyber Criminology,* (Choi, 2008); Reyns' article published in *Crime Prevention and Community Safety* situational crime prevention approach to cyber stalking victimization and preventative tactics for internet users and online place managers using opportunity theory and (Clarke, 1992, 1997) situational crime prevention (Reyns, 2010, p. 100); and Bossler and Holt's online activities and malware infection and guardianship using routine activity theory to explore victimization of data loss of college students and computer deviant malware making them targets (Bossler & Holt, 2009,p. 400-420). However, in the latter, both concurred that physical guardianship had little effect and that policy implications needed to decrease malware victimization in colleges could not focus on physical hardening (Bossler & Holt, 2009, p.400).

Retail stores. The online environment for credit card fraud contrasts greatly with that of the physical retail store, yet credit card fraud prevails in these environments as well. A review of consumer misbehaviors reported in Journal of Business Research (2004), discusses the profound impact of consumer misbehaviors and the effects it has on merchant employees within the retail store locations (Fullerton & Punj, 2002, p. 1239-1249). In fact, ABC News reported that those misbehaviors have subsequently had an impact upon how retail stores, especially large department stores, such as Walmart, Target. BestBuy, JC Penny's and Macy's conduct their costs and benefits analyses, chalking much of their loss to credit card fraud at the costs of doing business (Fahmy, 2010 as cited online at http://abcnews.go.com) These stores seem to be highly targeted for suitability of victimizing due to various reasons: 1) they carry hot brands and

popular electronics that can easily be liquidated for quick cash via the Internet or on the street, 2) they also allow consumers to purchase in-store gift cards using credit or bank debit cards, and 3) they are "known for their wide selection of goods and anonymity" they offer shoppers (http://abcnews.go.com). Most importantly, many large chains do not check customer cards for authorized signatures nor cardholder government issued picture identification bearing a genuine signature at point of sale terminals during checkouts. Neither do they check signatures for even limited visual comparison, relying solely upon data captured by electronic signature pads for fraud detection. This absence of POS checkout guardianship makes fertile soil for credit card fraud productions. Motivated offenders know this and take full advantage of the opportunities that these large retail chain merchants offer them, making those stores extremely suitable targets for credit card crimes. Here is an exemplary illustration of how routine activities theory applies to identity thieves utilizing someone else's credit or bank debit card and getting away with the fraud crimes because no one is acting as a capable guardian at POS terminals. There is a complete reliance upon new card securities, such as the EMV and e-pads to capture account information. As long as the payment is not declined, or a red flag does not go up alerting the employee that the card is stolen, then the consumer's misbehaviors—in this case credit/debit card fraud—has no repercussions. This reliance upon the electronic or digitized signature pad falsely replaces guardianship and can only help serve in fraud detection at a later point in time when the victim realizes charges to their accounts they did not make. If the fraudster has used counterfeiting equipment to manufacture fake credit cards using another person's active and viable account, then the event could be prevented if the POS employee would simply require cardholder picture identification at each transaction. According to FBI Agent Slotter, large-scale counterfeiting operations have developed in Taiwan, Hong Kong, and China, with smugglers

bringing in hologram materials into the US in California (Slotter, 1997, p.3). These fraudsters prey on victims worldwide due to the absence of capable guardianship in obtaining valid account information, usually online or in organized crime rings, and then make counterfeit credit cards and go on shopping sprees buying huge amounts of name brand items for resell on the streets. No one knows who they are targeting for account information, but it is easy to see why they are targeting large retail chains at which to shop, which many are international corporations making overseas access viable.

This research has involved in-store retail shopping with face-to-face transactions using four alternate cards in hand, to make both electronics and non-electronics related purchases in efforts to covertly investigate and observe the routine activities of cashiers with customers and potential fraudsters. The ultimate observation has been to determine if each specific cashier acted as either a capable or non-capable guardian at the POS terminals within three specifically targeted large retail chain stores, which are coded for privacy reasons. The goal was to gain understanding in search for particular themes or trends that are occurring causing the absence of capable guardianship at POS terminals within retail stores using the routine activities theory (Felson and Cohen, 1979). The development and implementation of the EMV chip technology within the United States has created a huge transition within the retail store POS terminal checkout environment. This researcher wished to observe first-hand how those changes were affecting merchants and their employees in daily routine activities of accepting credit or debit cards equipped with this new technology, and collectively analyze those observations to determine whether or not these merchants were being encouraged to act as capable guardians by adhering to the Visa and MasterCard guidelines set forth by the companies for card acceptance. Specifically, were the employees being required to adhere to the policy of securing identity at in-

store face to face transactions at POS terminals equipped with the EMV readers? What are the managers doing, if anything, to train their employees to check for proper authorized signatures and proper comparison of account numbers on the card versus that showing in the system?

Managers, acting as "super controllers" of these stores could thwart much fraud loss by requiring the cashiers to pro-actively assume the capable guardian role by offering employee incentives for fraud prevention, rather than simply writing off fraud loss as the cost of doing business. A great example of how this is implemented is in an essay prepared by a loss prevention employee for Tops Appliance City, Inc. located in New Jersey and New York, USA. Barry Masuda, of Tops Appliance, used in intelligence data to train store managers and employees how to "differentiate between legitimate from illegitimate" cardholder transactions (Masuda, 1991, p. 121). His efforts yielded a reduction of in-store credit card fraud from $1,121,000 in 1991 to $200,700 in 1992 by simple implementation of routine activity theory capable guardianship concepts (Cohen & Felson, 1979). Other theorists have applied rational choice, situated action and social control of organizations to retail store fraud crimes and argue that priority should be placed upon safety and the "well-being of the workers, consumers and general public" making it more challenging for effective guardianship (Vaughan, 1998, p.23). Sampson and Eck argue, in contrast, that not only should managers and employees act as guardians, but also act as "super controllers" (2010, p. 37). In their article, "Super controllers and crime prevention: a routine activity explanation of crime prevention success and failure," Sampson and & Eck raise awareness as to why people and organizations take (or fail to take) preventative action against crime (Bowers & Johnson, 2006; Laycock, 2006; Knutson, 2006 all as cited in Sampson & Eck, 2010, p. 37). This article effectively expands routine activity theory (Cohen & Felson, 1979; Felson, 2008) to "look at what influences people and organizations to

take crime prevention action" and conclude that "crime concentrations imply the systematic failure of at least one form of controller" (Sampson & Eck, 2010, p.47). In other words, the crime of identity theft and credit and debit bank card fraud has continued to occur in certain environments, such as those of the large department stores, because there is massive failure to act as capable guardians or controllers of the environment, and make interception and prevention possible.

Summary of Literature Review

Based upon the review of material within this paper, there is an obvious need for redefining capable guardianship. As demonstrated through various applications manipulating many elements of identity theft and credit and bank debit card fraud, it is equally obvious that R.A.T., or Routine Activities Theory (Cohen & Felson, 1979; Felson, 2008; Felson & Clarke, 1998) is the most applicable criminology theory for explaining this phenomenon. The absence of capable guardianship that evades and prevails over fraudulent financial transactions of these kinds needs serious study and research for future policy implications. A dominant theme throughout the context of this research paper is that of incapable and/or absent guardianship allowing identity theft and credit card crimes to continue to grow by leaps and bounds, both within the cyber world and the real physical world. Conquering this problem will require new methods of guarding information and transactions. Identity theft and credit and debit card fraud abound despite the implementation of laws, policies and even new EMV chip technology. The retail, restaurant and in-store face to face card in hand transactions are at optimal risks despite the merchants and employees' ability to properly identify each card paying customer at POS terminals. Observational field study research is warranted to discover causes as to why this phenomenon continues to occur.

CHAPTER 3

METHODOLOGY

Purpose of Research Restated

The purpose of this research is to investigate by first-hand field observations the absence or presence of capable guardianship at point-of-sale (POS) terminals within retail store chains that are known to be highly targeted for identity theft in conjunction with credit, debit or bank card fraud. (See pages 61- 62 of this thesis). A majority of bank cards bear the logo of either Visa or MasterCard. Both Visa and MasterCard mandate certain rules and regulations to be followed by merchants and their employees as outlined by their merchant agreement contracts (See Appendices C & D). Banks also have their own specific rules and regulations that are to be adhered to in order for the merchant to accept the card bearing the Visa or MasterCard logo for payment (See Appendix B).

Specifically, these rules require that each card must bear the legal cardholder's genuine signature on the back of the card within the signature strip that is located below the magnetic stripe and beside the security CVV code. Either above or below each signature strip located on the back of each card, are the words that read, "AUTHORIZED SIGNATURE – NOT VALID UNLESS SIGNED" (See Appendix C). Point-of-sale face-to-face transactions that occur within retail stores, with card in hand customers, are considered by both Visa and MasterCard to be the least risky transactions of all because the merchant's employees have the opportunity to investigate the identity of the customers paying with a plastic card method, and are required to do so if the card is not signed. The steps that the employees must follow at the POS terminal during the transaction are outlined by Bank Rules, Visa, and MasterCard (See Appendices B, C, & D for details). This investigator believes that the responsibility of acting as a capable guardian

that is placed upon the merchant and its employees is one that is often neglected and dismissed, thus it is also a contributing factor to the increase of identity theft related to card fraud.

Review of Research Questions Addressed and Hypotheses

Specifically, the following questions were addressed and hypothesized:

RQ1: The first research question contains five parts: 1) Will the cashier at the point of sale transaction act as a capable guardian over the face-to-face transaction and act to help prevent identity theft and credit/debit card fraud by taking the card into his or her hand to visually check the back of the credit or debit card to see if it bears an authorized signature by the legal cardholder, or check the account number on the card and compare it to that in the system or receipt in according to the merchant agreement rules as mandated by the Bank Rules and Regulations, Visa and MasterCard? (See Appendices B, C, & D). Variables investigated:

2) Will the variables of non-electronic versus electronic purchase increase levels of capable guardianship? Will there be a difference in the level of capable guardianship if the purchase is made at the back electronic counter POS terminal versus the store's front end POS terminal? 3) Will the amount of higher purchase charges to the card raise levels of guardianship at POS terminals with electronic purchases compared to a low levels of guardianship for small charges to the card? 4) Will the variables of time segment of day or night and business or lack thereof give increase or decrease to the levels of capable guardianship? 5) Will there be a difference of levels of guardianship based upon gender or race of the employee processing the transaction at each POS terminal?

Ho1: There will be an overall generalized absence of capable guardianship at the POS terminals during the face-to-face card in hand transaction, and the cashiers will not act as a

capable guardians over the card accounts in keeping with Bank Rules, Visa and MasterCard merchant agreement contracts in efforts to prevent identity theft. They will not take the card in hand at any point during the transaction to specifically compare the account number listed on the face of the card to that showing in the system nor will the cashier specifically check the back of the card to see if it has been validated by an authorized signature. Variable Hypotheses: 2) There will be a slight to significant difference between levels of guardianship when the purchase is an electronics purchase versus a non-electronic purchase or whether the purchase was made at the store's front end register or back electronic counter register. 3) There will be a higher level of capable guardianship demonstrated by participants at POS terminals when the charges to the credit card are over $50 versus those under $50. 4) There may be a slight difference in higher levels of guardianship depending upon the business of the store or lack thereof. 5) There will be no difference if the cashier is male nor female, Black or White. Overall, there will be a generalized absence of capable guardianship at the POS terminals within each store chain by all participants, with higher levels of guardianship being demonstrated only by those participants processing electronics purchases.

RQ2: Will the cashier at the face-to-face transaction at the POS (point-of-sale) terminal require the cardholder and purchaser to sign the back of the unsigned card used for purchase, and will he or she make her show a government issued photo identification for verification of her identity before the transaction is allowed to be processed through, in keeping with merchant agreement rules as mandated by Bank Rules and Regulations, Visa and MasterCard?

Ho2: The cashier will not check the back of the card, and therefore, will not check for an authorized signature validated the card. Consequently, the cashier will neither ask her to show a government issued photo identification document bearing her genuine signature for comparison

or verifying her identity before the transaction will be allowed to be processed through to its entirety. Ultimately, it is hypothesized that the cashier will not abide by the Bank Rules and Regulations, the Visa merchant rules for accepting unsigned cards, nor the MasterCard rules for accepting unsigned cards (See Appendices B, C, & D for references).

RQ3: Will the cashier act in lieu of an FDE (Forensic Document Examiner) to investigate by visual comparison the general similarities or differences of handwriting demonstrated on the government issued photo identification bearing a genuine signature of the researcher to that of the unsigned card that should be required to be signed in the presence of the cashier at the POS terminal?

Ho3: The cashier will not check the back of the card, and therefore, will not check for an authorized signature validating the card; thus, he or she will neither attempt to ask the researcher to sign the back of the card nor show government photo identification bearing her genuine signature, nor will he or she act in lieu of an FDE to investigate by general visual comparison the general similarities or differences of the handwriting on the government issued identification to that of the signature on the back of the card per requested signature. The cashier will not request a signature on the back of the card, and the only signature requested will be that prompted by the electronic signature capturing device at POS terminal.

RQ4: Will the cashier rely solely upon the electronic capturing device to verify the signature and not personally look at it himself or herself?

RQ5: Will the participant cashier at the POS terminal solely depend upon the EMC chip reader technology newly implemented at the POS terminals equipped with such to "guard" over

the identity of the cardholder, even when neither a PIN number nor signature is required nor requested for the transaction to be processed?

Ho4 and Ho5: The cashier participant processing the transaction will demonstrate heavy reliance upon the electronic signature capturing device, if a signature is required, and/or the EMV chip reader technology to "guard" over the face-to-face card in hand sales transaction at the POS terminal, whether a PIN is requested or required or not.

Procedures for Collecting Data

Gaining access to each of the 28 stores has been achieved by searching the Internet and obtaining a computer generated list of these three chains' store locations within the tri-states of Tennessee, Virginia, and North Carolina. A narrower list has been accumulated be sectioning each state off into bordering regions and searching for store locations within those specific regions of Eastern Tennessee, Western Virginia, and Northeastern North Carolina and choosing those that were randomly located along the I-81, I-40, I-75, and I-26 interstate highways. Stores were randomly selected for patronizing along each individual interstate highway. Shopping dates consisted of a busy six day period from February 12 through February 17, 2016. This was a long holiday weekend consisting of Valentines' Day, Saturday, February 14th and President's Day, February 16th. Data was collected by observational studies made during thirty-four (34) separate transactions at these twenty-eight (28) different store locations randomly selected for shopping. The researcher alternated between purchasing an electronic related item and paying for it at a POS terminal located in the back of the store in the electronics department, and purchasing less expensive non-electronic items from the POS terminals located at the front of the department store. The purchase amounts ranged from$1.41 (food item) to $246.07 (LG Stereo). Receipts were saved and an observations report was filled out immediately upon leaving each

individual store and after each individual transaction occurred to collect and code certain data (See Appendix A). The construction of the observations report is discussed further at the end of this chapter. Ideas and evidence that supports hypotheses as to the absence or presence of capable guardianship existing at POS terminals at these specific department stores emerged from the field based upon the accumulative observational studies.

Four separate plastic card payment methods were utilized by the researcher as the legal cardholder and consumer, but all of the signature strips on the backs of these four cards were entirely unsigned, therefore not valid to be used for purchases unless signed in the presence of the employee at the POS terminal. Two of the cards bear the logo of Visa, while the other two bear the logo of MasterCard. Two of the cards were encrypted with EMV chip technology but also had magnetic stripes; while the other two had security features of magnetic stripes and PIN numbers. In addition to observational data collected during thirty-four (34) separate face-to-face card in hand transactions at thirty-four separate POS terminals with thirty-four separate individual employees occurring within twenty-eight (28) different stores, basic demographics were also collected regarding the gender, race, and time segment of the day or night, including: 6 am – 12 noon; 12 noon- 6 pm; 6 pm-12 midnight; 12-midnight – 6 am. These variants were charted to help determine if there was a difference in the employees' adherence to the store's merchant agreement policy depending upon gender, race or the time of day each individual transaction occurred correlating with the business or lack of business inside the store.

Store Chains and Coding

There were three individual national store chains selected for this research. Two were chosen based upon their sales and easy access to both electronic products and non-electronics related items. One was an electronics department store only, but sold inexpensive accessories

also. All three are large national chains predominantly located within the United States of America. Some of these chains are also located internationally and called by different names, although they are still owned by the associates of the same companies located within the U.S. All three store chains were also known to be reported as highly targeted for identity theft and card fraud. To protect the privacy of each individual store chain and location and to prevent incrimination of individual employees of these three individual store chains, a coding system has been implemented. For this reason, the three chains have been coded as Store Chain #1, Store Chain #2, and Store Chain #3. No specific information has been reported on the individual store names nor locations in the observations reports (See Appendix A). Locations have been coded within each individual state where each store was located and each transaction occurred, and the choices included those states within the region investigated: Tennessee, North Carolina, Virginia or Georgia.

Participants at POS Terminals

Furthermore, no personal identifying information has been collected on specific employees at POS terminals, nor has it been discussed in this research thesis. Participants of these three individual store chains were required to be over the age of eighteen in order to be eligible for employment at each store, due to its being a national chain; therefore, all participants at POS terminals were considered adults for research purposes. The participants were randomly chosen by location of the POS terminal in which the purchase was being made, and the participant was working. Thus, if the item was considered to be an electronics related item, then the researcher sought to process the transaction at the electronics POS terminal normally located in the back each store in the electronics department. If the item purchased was considered to be a non-electronics related item, then the researcher sought out a POS terminal

located at the front of the store to process the face-to-face transaction. The participants at the front POS terminals were chosen by randomly noting which terminal had the shortest line at the time the sales transaction occurred. The demographics of gender and race only of each participant were recorded on the Observations Report (See Appendix A).

Purchases

Thirty-four (34) individual purchase transactions occurred at thirty-four (34) individual POS terminals. The goal was to purchase as many non-electronics related items that were inexpensive and compare the observations to the near equivalent number of electronics related items purchased that were more expensive. The purpose of this distribution was to observe the differences in the guardianship levels initiated by the participants at the POS terminals during each electronic or non-electronic related transaction. Most electronic transactions have certain stipulations that require added security. For example, electronics items must be returned within fourteen (14) calendar days versus the usual thirty to ninety days, as stated on receipts and as determined by each individual store chain policy.

Electronic items are also highly targeted by identity thieves and fraudsters because they are high in demand and easy to liquidate either on the street or online, according to the statement of the problem and the research cited in the literature review of this thesis (See Ch. 1 & Ch. 2 for references). For this reason, some electronics items are placed within locked security cases or are locked down on the shelves with security cables, and require the assistance of a sales associate, who subsequently often acts as the cashier at the POS electronics terminal. All of these measures are taken in efforts to help prevent stolen merchandise from leaving the merchant's store. It was hypothesized by this researcher that there would be higher levels of guardianship

by the participants at POS terminals located at the electronics counters at the back of each store specifically used for processing electronics related purchases (See Ho1).

Payment Methods and Security Features of Cards Used

Four individual credit/debit cards were utilized for the thirty-four (34) individual transactions. They were not used in equal distribution, but selected and used in unequally distributed proportions. The reason being: Two of these plastic payment cards were encrypted with the new security feature introduced into the U.S. based upon the European model of the EMV chip and pin technology. The two other cards consisted of features of the magnetic stripes only as a method of being read for transaction processing. The researcher determined after visiting the first three stores in each one of the respective chains, that they were making or had already made the transition to technology equipped to read the EMV chip in the card. That said, the researcher made the rational choice to primarily observe and test the guardianship levels of participants at POS terminals equipped with the new readers as mandated by the EMV Liability Shift that occurred as of October 1, 2015 by Visa's, MasterCard's, American Express's and Discover's rules (See p. 26-27 in Ch. 1's Definition of Terms). Since only two of her credit cards were encrypted with the new EMV chip card technology, she opted to utilize these for most purchases despite that they were both bearing the MasterCard logo. The two bearing the Visa logo were utilized least, because neither were yet encrypted with the EMV chip technology.

Construction of Observations Report

The construction of the observations report (See Appendix A) was based upon several criteria that were intended to be observed and recorded by the researcher during her field studies and transactions as an American card paying consumer. These criteria included the following: 1) the code for each store chain and state in which it was located, 2) the time that actually

transaction took place coded into a category of one to four segmenting the twenty-four (24) hour cycle of each date, 3) the demographics of gender and race only of each individual participant at each POS terminal transaction occurred, 4) the location of each individual POS terminal specified in front of store for general purchases and in back of store for electronics related purchases, 5) whether the item purchased in each transaction was electronics related or non-electronics related, 6) the amount of charges incurred on each specific card utilized for each transaction, 7) the individual security features that were utilized by the technology equipped at each POS terminal, 8) the individual level of guardianship initiated by the participants processing the sales transaction at each POS terminal. Additional information and notes were obtained and recorded if warranted by normal daily activities routine conversations occurring during the transaction process.

Coded Chain Store Location and Number (#)

Three specific national retail store chains were patronized for shopping with an accumulative totaling twenty-eight (28) individual store chains visited by the researcher as a consumer making face-to-face card in hand transactions. Each store and location was coded as either being "Store Chain #1, Store Chain #2, or Store Chain #3," for privacy purposes. Attempts were made to patronize each of the specific store chains #'s 1-3 in somewhat equivalent proportions, depending upon accessibility within each state in the region investigated. The location of each store was classified according to the state in which the business was located, and the choices were: Tennessee, Virginia, North Carolina and Georgia.

Time Segments Transactions Occurred

Time segments were categorized as occurring within one of the following: 1) Segment 1—meaning the transaction time fell between 6:00 a.m. and 12:00 noon, 2) Segment 2—

meaning the transaction time fell between 12:00 noon and 6:00 p.m., 3) Segment 3—meaning the transaction time fell between 6:00 p.m. and 12:00 midnight, or 4) Segment 4—meaning the transaction time fell between 12:00 midnight and 6:00 a.m. Exact times of transactions were not recorded in efforts to protect the cashier participants' personal identifying information from being revealed as receipts record exact times and names of cashiers and/or numbers of exact POS terminals transactions occur. All efforts were made to prevent any personally incriminating information to be reported on the observations report sheets (See Appendix A). Meanwhile, times were categorized into quarterly segments to demonstrate any differences in levels of guardianship efforts made by POS cashiers during non-busy shopping hours as compared to busy shopping hours. According to *Visa's Card Acceptance Guidelines for Visa Merchants* rules located in Section 2: Card-Present Transactions, merchants are to train their employees to be aware of card transactions made specifically right after the store opens and/or just before the store closes as these times tend to be when much fraud occurs (p. 35). This also indicates the store's being busy or not busy. Usually stores are not very busy as soon as the store opens or just before it closes as most customers do not patronize stores immediately upon opening nor closing.

Demographics of Participants at POS Terminals

The demographics of participants records only the gender and race of each cashier that processed each transaction. The purpose of recording gender was to determine if there were differences in levels of guardianship dependent upon sex. For example, if the cashier were a male versus a female, would natural guardianship instincts or efforts be greater, or vice versa. The purpose of recording race was determine if race was a contributing factor in awareness of identity theft and card fraud, and thus vigilance or lack of vigilance in practices of higher or

lower levels of guardianship at retail store POS terminals in efforts to prevent it. One study cited earlier in this thesis in Chapter 2, Literature Review stated that Black African American women targeted White Caucasian males as victims (See pages 43-44 of this thesis).

Location of POS Terminal within the Stores

Each POS terminal location was recorded as either being located at the back of the store in the electronics department being located at the front of the store. Back of store electronics POS terminals were utilized primarily for sales transactions involving electronics related items; while front of store POS terminals were utilized primarily for sales transactions involving non-electronics related items. Depending upon the time segment category in which the purchase was made, there was either adequate employees staffed to access both types of POS terminals, or only front of store POS terminals, if employee staff numbers were low during certain shopping hours. The purpose in recording the POS terminal location as either back of store electronics or front of store general was to determine if there were differences in efforts and levels of capable guardianship by participants at each type of terminal, based upon training and requirements for those operating the POS terminals pertaining to electronics purchases compared to training and requirement for those operating POS terminals used for general non-electronic purchases.

Electronic vs. Non-Electronic Items

Each individual transaction was recorded as either being an electronics related item meaning it was sought out and obtained from the electronics department of the specific retail store, or it was recorded as being a non-electronics related item. The purpose of recording whether the item purchased by card payment method was either electronics related or non-electronics related was to determine the differences in guardianship efforts made during the face-to-face card in hand in store sales transaction if the item was an electronics related item versus a

non-electronics related item. According to the review of the literature cited in Chapter 2 of this thesis, electronic items are highly targeted by identity thieves and card fraudsters because these items are in high demand and are easily liquidated either on the streets or online (See page 62). It stands to reason that guardianship efforts would be assumed to be greater for electronic purchases, and it was hypothesized that they would be (See page 69). In order to test this hypothesis, it was required to record whether each individual item was electronics related or non-electronics related.

Amount of Charges to Specific Card Used

The exact amount of each charge applied to each card account was recorded on the Observations Report for each individual transaction. The purpose of recording each exact amount was to document any differences of efforts of guardianship providing the charges were higher in amount compared to lower in amount. It was assumed and hypothesized that the higher charges would warrant higher levels of guardianship efforts by the participants at the POS terminals (Ho1). The amount of the specific charge related to each individual face-to-face card in hand sales transaction was a determining criteria as to whether or not the system required the researcher as cardholder and purchaser to provide an electronic signature on the capturing device. Retail stores often require a signature if the amount charged to the card is above a certain predetermined threshold. Conversely, a signature is often not required by a system whose threshold is set below a certain predetermined amount charged to the card. Charges were calculated accumulatively to each specific card made over the six (6) day shopping period.

Card Being Used for Transaction and Coding

A total of four individual credit/debit cards were utilized in unequal distribution for all accumulative transactions. Reasons for unequal distribution of card use is discussed in depth in

the previous section entitled, "Payment Methods and Security Features of Cards Used," (See pages 73-74). Primary criteria recorded on the observations reports notated if the card itself bare either Visa's or MasterCard's logo, as these were the only two types accounts of which the researcher had legal ownership. Two of the cards used were Visa, while the other two were MasterCard. The two Visa cards were equipped with magnetic stripes only, while the two MasterCard cards were encrypted with magnetic stripes and EMV chip technology newly introduced into the US and able to be read by merchants who have made the transition to use POS terminals equipped with EMV chip readers, per the EMV liability shift requirement as of Oct. 1, 2015. The researcher's legal name and card account number, as well as expiration date were on the front of each card, along with the logo; and on the backs of each card were security CVV codes located next to the blank signature strips. The researcher did not sign any of these four cards to make the cards "valid" for purchases as mandated by Visa and MasterCard rules and regulations: "AUTHORIZED SIGNATURE – NOT VALID UNLESS SIGNED," in bold capital letters above or below each unsigned signature strip (See Appendices C & D). The security features of each card were noted on the observations reports as well as the specific card that was used. However, the last four digits printed on each sales transaction receipt were renumbered for privacy purposes and coded as either ending in "1111," "2222," "3333," or "4444."

Guardianship Efforts of Participant Employees

The questions asked on the observations report regarding the guardianship efforts of each individual participant employee at each POS terminal addressed the following : 1) Did the cashier take the credit/debit card in hand to check anything at all, including but not limited to the account number or CVV code? 2) Did the cashier notice and state that the card was not signed

to the researcher as card paying customer? 3) If so, did the cashier ask her to sign the card in the cashier's presence as mandated by merchant agreement contracts and bank rules (See Appendices B, C, & D). 4) If the cashier requires the unsigned card to be signed in his or her presence, does he or she sequential ask the card signer, researcher and card paying customer to provide her government issued photo identification bearing her genuine signature for comparative purposes? 5) If all those steps are followed properly, does the cashier demonstrate efforts to visually compare and contrast generally visible differences, in lieu of a trained FDE, between the newly signed signature located inside the signature strip on the back of the previously unsigned card to that of the genuine signature located on the government issued photo identification provided to the cashier? 6) Were there any additional guardianship efforts demonstrated by the cashier, such as calling for Code 10, if she believed there to be discrepancies or reasons to be suspicious of fraud (Based upon guidelines from MasterCard's *What If Fraud Happens*, p. 1)? Any additional efforts were noted in the blanks lines of "Additional" on the Observations Report (See Appendix A).

Technology Used in Transactions

The technology utilized for each transaction to be completed was recorded as follows: 1) Did the system used at the POS terminal during the face-to-face card in hand sales transaction request for an electronic signature to be captured by the device? 2) Did the system require the EMV chip reader to read the account information encrypted into the EMV chip on the card being used (if card used was equipped with EMV chip technology) or simply slide the magnetic stripe to read the account information? 3) Did the system prompt for a PIN number to be input before the transaction could be completed? 4) Did the cashier demonstrate by conversation the deference of guardianship to the EMV chip reader or to the electronic signature capturing

device? If so, the words of the cashier were noted in the additional observations section, as described below.

Additional Notes and Observations

This section of the Observations Report consisted of blank lines to record any additional information observed or collected as data for research purposes. This included but was not limited to normal conversations made during the daily routine activities of shopping, checking out, and paying with a credit or debit card. If the participant cashier at the POS terminal offered any comments or statements during the transaction, specifically regarding the new EMV chip reader and technology, they were documented and reported in this section. Any other information or observations the researcher believed to be pertinent to this study were also recorded in this section and analyzed for any recurrent themes or trends by accumulative comments representing recurrent ideology.

CHAPTER 4

RESEARCH FINDINGS

A total number of twenty-eight (28) individual major department stores combined, located within Tennessee, Virginia, North Carolina and Georgia were patronized as a normal paying customer and observational studies were made during a total accumulation of thirty-four (34) point of sale purchase transactions with thirty-four (34) individual cashiers, involving the payment method of plastic credit/debit cards, with actual amounts ranging from the least expensive (food) purchase of $1.41 to the most expensive (LG stereo) purchase of $246.07. The least expensive purchase of $1.41 was made at store chain #2 using a MasterCard credit card with chip technology without using a pin nor signature, while the most expensive purchase of $246.07 was made at store chain #3, using a different MasterCard credit card with chip technology and electronic signature only, with no pin number required. These thirty-four (34) individual transactions were made over a six (6) day period from Friday, February 12, 2016 – Tuesday, February 17, 2016 using four (4) different major credit/debit cards, two of which were MasterCard and two of which were Visa. None of these four major credit cards were signed with any mark or signature anywhere on the cards, by the legal cardholder and purchaser nor anyone else, specifically inside the white strips on the back of the cards provided above or below the captions on each stating, "AUTHORIZED SIGNATURE – NOT VALID UNLESS SIGNED." A total combined amount of $1,730.48 was spent during this six (6) day shopping spree at twenty-eight (28) different stores within Tennessee, Virginia, North Carolina and Georgia, accumulating thirty-four (34) different sales transactions with thirty-four (34) different cashier participants within three (3) separate large department store chains that sell electronics—items commonly targeted for theft.

Distribution of Store Chains

Table 1

Region of Coded Store Chains Patronized for Observational Studies

(28 Stores Visited in Total)

Store Chain Code Number	Tennessee	North Carolina	Virginia	Georgia	Total # of Stores Visited
#1	11	2	1	1	15 **(54%)**
#2	4	2	1	0	7 **(25%)**
#3	3	2	1	0	6 **(21%)**
All Stores Combined	18 **(64%)**	6 **(21%)**	3 **(11%)**	1 **(4%)**	28 **(100%)**

Distribution of Participants

The researcher selected participant stores from each one of the three major chains of high volume sales department stores for observational studies during purchases, based upon the convenience and accessibility of the store locations to the interstates (I-81, I-40, and I-75) within the Tri-State region and near state lines of Tennessee, Virginia, North Carolina and Georgia. The participant stores are coded as Chain #1, Chain #2, and Chain #3 depending upon the frequency of their occurrences along the interstates route and largest to smallest number of stores visited. The total number of stores and purchases made at Chain #1 in this region combined accumulative was twenty (20) individual purchases utilizing twenty (20) individual cashiers for point of sale transactions made at fifteen (15) different store locations within Chain #1. The total number of stores and purchases made at Chain #2 in this region combined accumulative was eight (8) individual purchases utilizing eight (8) individual cashiers for point of sale transactions

made at seven (7) different store locations within Chain #2. The total number of stores and purchases made at Chain #3 in this region combined accumulative was six (6) individual purchases utilizing six (6) individual cashiers for point of sale transactions made at six (6) different store locations within Chain #3.

The individual cashier participants were all legally adults of eighteen years of age or older based upon each chain's employee minimum age requirements for hiring. Each front register cashier was randomly chosen by availability or convenience of the line length based upon the business of each store visited. Each electronics counter cashier was chosen by convenience of who was working there at the time of purchase. In some stores, it was difficult to find anyone working at the electronics counter and front register cashiers were randomly and conveniently utilized for electronic purchases that did not require an attendant to remove them from behind a locked glass security case. Other cashier participants were chosen randomly by whom arrived when the bell at the electronics counter was rang asking for customer assistance to retrieve items locked in glass security cases and complete point of sale purchase transactions. Both male and female participants were randomly selected by convenience. These male and female participants randomly included whites and blacks. There were a total number of sixteen (16) male cashier participants, of which three (3) were black and thirteen (13) were white. Alternately, there were a total number of eighteen (18) female cashier participants, of which four (4) were black and fourteen (14) were white. There were a total of fourteen (14) female cashiers, of which three (3) were black and eleven (11) were white: and, six (6) male cashiers, of which zero (0) were black and six (6) were white at store Chain #1. There were a total of three (3) female cashiers, of which one (1) was black and two (2) were white: and, five (5) male cashiers, of which zero (0) were black and five (5) were white at store Chain #2. Finally, at store Chain

#3, there was a total of one white (1) female cashier that assisted point of sale transaction, and five (5) male cashiers, of which three (3) were black and two (2) were white. All stores combined equals thirty-four cashier participants, eighteen (18) females and sixteen (16) males randomly chosen by convenience. These are the only demographics obtained pertaining to individuals logged for research purposes, and no further personal identifying information was gathered during these observational studies in order to protect the privacy and PID of each individual cashier participant during each point of sale transaction. The purpose in documenting the demographics of male versus female, as well as black versus white, was to determine if there is a consistent difference in point of sale practices during transactions involving plastic card payments of MasterCard or Visa in either's adherence to merchant agreement policies for checking for authorized signature on back of card and requiring government issued identification if the card is not signed.

Table 2

Demographics and Numbers of Participants:

Gender and Race of Cashiers at POS Terminals, Face-to-Face Transactions

Store Chain	Females	Males	Totals	Caucasian Ethnicity	African American Ethnicity	Totals
#1	14	6	20	17	3	20 (**59%**)
#2	3	5	8	7	1	8 (**24%**)
#3	1	5	6	3	3	6 (**18%**)
All Stores Combined	18 **(53%)**	16 **(47%)**	34 **(100%)**	27 **(79%)**	7 **(21%)**	34 **(100%)**

Distribution of POS Terminals

Table 3

POS (Point-of-Sale) Terminal Locations within Stores Utilized for Face-to-Face Transactions

POS Terminal Location in Store Chain	Electronics Counter in Back of Store	Counter in Front of Store	Total Combined Locations
#1	10	10	20
#2	3	5	8
#3	2	4	6
All Stores Combined	15 **(44%)**	19 **(56%)**	34

Purchases and Data Analysis Strategy

The total amount of thirty-four (34) combined accumulative purchases was $1,730.48 at all three store chains, #1, #2, and #3—all made with credit/debit card payments in a five (5) consecutive days period. Broken down, $787.64 was spent during transactions using a payment method of plastic credit/debit card at Chain #1; $261.01 at Chain #2; and $681.83 at Chain #3; finally, $50.55 at Chain #4. The purchases varied in amounts ranging as low as $1.41 to as high as $246.07, with the average purchase price amounting to $50.89. This figure was obtained by calculating the total of $1730.48 of all combined purchases divided by 34, the number of total transactions. Specifically, there were twenty-three (23) purchases made that were under $50.00 each and eleven (11) purchases made that were over $50.00 each.

The purchases were all made over a busy long weekend and shopping holiday of Valentine's Day weekend (Sunday, February 14, 2016) and President's Day (Monday, February 15, 2016) while children were out of school and many parents were given a day off at work.

Additionally, this period is also when many people are receiving their tax refunds and shopping capacity is at its peak volume. Also, purchases were made at different times of the day and night hours to observe any discrepancies in cashiers' adherence to merchant agreement policies of credit/debit card payments to either check for authorized signature and government issued photo identification or not, due to busy hours and long lines, versus least busy hours and no lines. Specifically, each segment of the twenty-four (24) hour cycle was broken down into four categories as follows: 12:01 am midnight to 6:00 am as segment 1; 6:01 am to 12:00 noon as segment 2; 12:01 noon to 6:00 pm as segment 3; and 6:01 pm to 12:00 midnight as segment 4. There were a total number of two (2) purchases made during segment 1, which was the least busiest time for shopping; seven (7) purchases made during segment 2, which was a moderately busy time for shopping; fourteen (14) purchases made during segment 3, which was the busiest time overall for shopping; and eleven (11) purchases made during segment 4, which was a moderately busy time for shopping.

Of the thirty-four (34) purchases made, fifteen (15) of them were made at each store's electronics counter located in the back near the electronic item purchases; while nineteen (19) of them were made at a front register either because the item purchased was not an electronic item, or no one was available at the back electronic counter to assist in the point of sale transaction. The purpose in choosing electronic counter cashiers versus front register cashiers was to observe any differences in cashier's adherence to merchant agreement policies when payments involved a MasterCard or Visa credit/debit card transaction. Also, being observed were differences in store practices of security measures in point of sale transactions made at electronic counters for electronic items commonly targeted by thieves, versus other store items not as commonly targeted. Specifically, ten (10) electronic purchases were made at the electronics registers in

back of store Chain #1, three (3) electronic purchases were made at the back electronics registers at store Chain #2, and two (2) electronic purchases were made at the back electronics registers at store Chain #3. Ten (10) non-electronic purchases were made at front registers of store Chain #1; four (4) non-electronic purchases and one (1) electronic purchase was made at the front registers of store Chain #2; zero non-electronic related purchases were made at store Chain #3 (it is an all electronics chain store), but six (6) electronic related purchases were made at store Chain #3, of which two (2) occurred at back registers near the large items purchased –one being a 32" flat screen television with a built in Roku box and the other being an LG 700W stereo system—and four smaller items purchased (4) occurring at front registers. Total number of electronic purchases at all stores combined was twenty (20). Total number of non-electronic purchases combined at all stores was fourteen (14). One purchase made at the electronics counter was not electronics items but rather dog food, candy and clothing. Whereas, several (at least five) electronic purchases were made at front registers versus back electronic counters for various reasons, primarily lack of cashier assistance available at back electronics department registers.

Table 4

Time Segments when Purchases Were Made

Store Chain# (Coded)	**Segment 1 (12:00 am – 6:00 am)**	**Segment 2 (6:01 am- 12:00 pm)**	**Segment 3 (12:01 pm – 6:00 pm)**	**Segment 4 (6:01 pm – 11:59 pm)**
#1	2	5	8	5
#2	0	1	3	4
#3	0	1	3	2
All Stores Combined	2 **(6%)**	7 **(21%)**	14 **(41%)**	11 **(32%)**

Table 5

Itemized List of 34 Purchases, Charges Incurred, and Technology Used for Transaction

(Arranged in alphabetical order)

Item Purchased	**Store Chain *(Coded)***	**Electronic or Non-Electronic**	**Amount Charged to Card**	**Card Used For Purchase *(Coded)***	**EMV Chip**	**PIN**	**Magnetic Stripe**	**Electronic Signature Required**
32" Flat screen TV	3	Electronic Item	$240.73	MasterCard 2222	Yes	No	No	Yes
Bananas and Vitamin Drink	1	Non-Electronic Items	$2.76	MasterCard 1111	Yes	No	No	No
Bathroom Tissue	1	Non-Electronic Item	$9.85	MasterCard 2222	Yes	No	No	No
Beats Headphones	2	Electronic Item	$116.62	MasterCard 2222	Yes	No	No	Yes
Birthday Cards	1	Non-Electronic Item	$6.50	MasterCard 1111	Yes	No	No	No
Black Light Bulb	2	Non-Electronic Item	$5.86	MasterCard 1111	Yes	No	No	No
Camera Tripod, DVD	2	Electronics Related Item	$57.05	MasterCard 1111	Yes	No	No	Yes
Canon Camera Bag	3	Electronic Related Item	$23.49	MasterCard 1111	No	No	No	No
Canon Photo Printer + Glossy	3	Electronic Item	$150.01	Visa Debit 3333	No	Yes	Yes	Yes
Cat Food, Bottled Water	1	Non-Electronic Items	$10.24	MasterCard 1111	Yes	No	No	No
Chips, Gum	1	Non-Electronics Item	$4.67	MasterCard 2222	Yes	No	No	No
Composite AV Cable	1	Electronics Related Item	$10.49	MasterCard 1111	Yes	No	No	No

Item Purchased	Store Chain (*Coded*)	Electronic or Non-Electronic	Amount Charged to Card	Card Used for Purchase (*Coded*)	EMV Chip	PIN	Magnetic Stripe	Signature Required
DVD	2	Electronics Related Item	$5.49	Visa Debit 3333	No	Yes	Yes	No
DVD/VCR Combo	1	Electronic Item	$113.25	MasterCard 2222	Yes	No	No	Yes
DVD's	1	Electronics Related Items	$13.87	Visa-Debit 3333	No	Yes	Yes	No
Energizer Rechargeable Battery Pack	1	Electronics Related Item	$20.82	MasterCard 2222	Yes	No	No	No
Ethernet Inline Coupler	3	Electronics Related Item	$10.94	MasterCard 2222	Yes	No	No	No
Fireproof Security File	2	Non-Electronic Item	$69.52	MasterCard 1111	Yes	No	No	Yes
Flat Screen TV Wall Mount	1	Electronics Related Item	$95.13	MasterCard 1111	Yes	No	No	Yes
Generic Acetaminophen	2	Non-Electronic Item	$3.27	MasterCard 1111	Yes	No	No	No
Gloves	1	Non-Electronic Item	$4.38	MasterCard 1111	Yes	No	No	No
Gum, Dasani	2	Non-Electronic Items	$3.09	MasterCard 1111	Yes	No	No	No
LG 700W Shelf Stereo	3	Electronic Item	$246.07	MasterCard 2222	Yes	No	No	Yes
Listerine Mouthwash	1	Non-Electronic Item	$6.54	MasterCard 1111	Yes	No	No	No
Magellan GPS	1	Electronic Item	$106.46	MasterCard 2222	Yes	No	No	Yes
Pillow, Dog Food, Shirt	1	Non-Electronic Items	$26.58	MasterCard 1111	Yes	No	No	No
Popcorn	2	Non-Electronic Item	$1.41	MasterCard 1111	Yes	No	No	No

Item Purchased	Store Chain (Coded)	Electronic or Non-Electronic	Amount Charged to Card	Card Used for Purchase (Coded)	EMV Chip	PIN	Magnetic Stripe	Signature Required
Princess Barbie	1	Non-Electronic Item	$9.88	MasterCard 1111	Yes	No	No	No
Samsung Android Cell Phone	1	Electronic Item	$206.14	MasterCard 1111	Yes	No	No	Yes
SanDisk 16GB Memory Card	3	Electronics Related Item	$10.91	MasterCard 1111	No	No	No	No
Straight Talk Phone Card	1	Electronics Related Item	$50.55	Visa 4444	Yes	No	No	Yes
Swimwear	1	Non-Electronic Item	$23.93	MasterCard 1111	Yes	No	No	No
Valentine Cards, Candy, Flowers	1	Non-Electronic Items	$37.51	MasterCard 1111	Yes	No	No	No
Xbox 360 Video Game	1	Electronics Related Item	$28.09	MasterCard 2222	Yes	No	No	No

Table 6

Electronics Related Purchases vs. Non-Electronics Related Purchases

(34 Combined Purchases in Total)

Number of Purchases Made at Store Chain	**Electronics Related Items**	**Non-Electronics Related Items**	**Total Combined**
#1	10	10	20
#2	4	4	8
#3	6	0	6
All Stores Combined	20 **(59%)**	14 **(41%)**	34

Credit Card Data Analysis and Coding

The total number of sales transactions involving plastic credit/debit card payments were thirty-four (34) combined accumulative at all store chains and from all transactions. Four different credit/debit cards were utilized where purchaser and observer both were the legal cardholder. Of these four, two (2) of the credit/debit cards were MasterCard accounts (both with new chip technology and magnetic strip slide capability) and two (2) were Visa accounts (slide only cards still without chip technology). For privacy purposes and maintenance of PID of the legal cardholder, these four credit cards will be coded as follows: The first credit/debit MasterCard account primarily used for twenty (20) purchases, encrypted with chip technology and magnetic slide strip will be coded as ending in 1111; the second credit/debit MasterCard account secondarily used for ten (10) purchases, also encrypted with chip technology and magnetic slide strip will be coded as ending in 2222; the third debit Visa account thirdly used for

only three (3) purchases, and not yet encrypted with chip technology but only has magnetic slide strip that requires a pin number to complete transactions will be coded as ending in 3333; and finally, the fourth credit Visa account lastly used for only one (1) purchase, and not yet encrypted with chip technology but only has magnetic slide strip that does not require a pin number will be coded as ending in 4444. None of the previously described and coded cards have been officially signed by the researcher and legal cardholder, nor any other person; therefore, the backs of each card are blank in the white strips provided for "Authorized Signature" and stated as "Not Valid Unless Signed" by the card issuer.

There were a total number of thirty-one point of sales transactions made with three credit cards coded above as ending in 1111, 2222, and 4444 that did not require a pin number for transactions to be completed by cashiers. The total amount of charges applied to MasterCard for combined twenty purchases was $613.06 on card coded as ending in 1111. The total amount of charges applied to MasterCard account for combined ten (10) purchases was $897.50 on card coded as ending in 2222. And the total amount of charges applied to Visa credit card account coded as ending in 4444 was $50.55. Two of these cards were equipped with chip technology (1111 and 2222), and one was slide only (4444). There were a total of three point of sale transactions totaling $169.37 combined that required a pin number and they were all involving the Visa debit card coded as ending in 3333, of which, the legal cardholder and researcher knew the correct pin number associated with this account. One transaction occurred at store Chain #1, one occurred at store Chain #2, and one occurred at store Chain #3—each being debit transactions. Zero (0) of the remaining thirty-one purchases made with credit cards equipped with chip technology or not (1111, 2222, and 4444), ultimately required a pin number to complete these in store point of sale transactions. (Add total combined purchase amount)

Two of those specific transactions, both made at store Chain #3 (where only electronic related items are sold) and both using MasterCard account coded as ending in 1111 and encrypted with chip technology, but also containing a magnetic slide strip were prompted by the electronic signature pad system to provide a pin number. However, when the researcher and legal cardholder told the cashiers at each store (one transaction involving a white female cashier, and one transaction involving a black male cashier) that she could not remember the pin number the system was prompting her for, each one offered to assist her by putting the account number in manually from another screen. Once the account number was properly entered manually, then the cashier was prompted to enter the three digit security code on the back of the card. Each cashier during each one of the two individual transactions at two different store locations within the region, held the card in their hand viewing the back of the card to see and enter the security code located at the end of the white strip on the back that is designated for the authorized signature. Both of these two cashiers had opportunity to see that the card was not properly signed and the white area was blank. They each also had opportunity to read the statement near the blank strip that read "Not Valid Unless Signed." Neither of the cashiers said anything to the legal cardholder and purchaser during the transaction about the need to sign her card nor their need of verifying who she was by asking to see her photo identification according to MasterCard's merchant agreement, since the card was not signed and authorized for use. Each one of these two cashiers at two different store locations of Chain #3 successfully completed the transactions for her manually without the need or use of a pin number as the electronic signature pad and system was requesting. Both of these transactions were made at front registers of this store chain. The amount of one purchase was $10.91 and the item was a SanDisk 16 GB Memory Card. The amount of the other purchase was $$63.17 and the item was a Canon Gadget

Camera Bag. This purchase involved $40.00 cash and $23.17 on MasterCard coded as ending in 1111. It is worth mentioning that these two individual purchases were made at busy shopping times of the day, with one purchase made at peak busy hours at 4:06 pm and the other at moderately busy shopping hours of 11:18 am.

Table 7

Total Charges Incurred at Each Store Chain from All 34 Transactions

Store Chain # (Coded)	**Charges Applied to Card "1111"**	**Charges Applied to Card "2222"**	**Charges Applied to Card "3333"**	**Charges Applied to Card "4444"**	**Totals**
#1	$440.08	$283.14	$13.87	$50.55	**$787.64 (46%)**
#2	$138.90	$116.62	$5.49	$0	**$261.01 (15%)**
#3	$34.08	$497.74	$150.01	$0	**$681.83 (39%)**
All Stores Combined	**$613.06 (35 %)**	**$897.50 (52%)**	**$169.37 (10%)**	**$50.55 (3%)**	**$1730.48 (Combined %'s = 100%)**

Table 8

Number of Sales Transactions Attributed to Each Card

Card "1111"	**Card "2222"**	**Card "3333"**	**Card "4444"**
20 (59%)	10 (29%)	3 (9%)	1 (3%)

Summary of Transactions

A summary of the thirty-four (34) individual transactions is as follows: twenty-eight different stores were selected accessed randomly by convenience along I-81, I-40, I-75, and I-26 within Tennessee, Virginia, North Carolina and Georgia for a combined accumulative of thirty-four (34) separate transactions involving thirty-four (34) separate individual cashiers who were also selected randomly based upon who was available at the register to assist my transaction at the time the transaction occurred, but were somewhat balanced between eighteen (18) female cashiers and sixteen (16) male cashiers. The times of these transactions took place and were coded within four segmented hours of the twenty-four hour cycle: 12:01 am-6:00 am; 6:01 am – 12:00 noon; 12:01 noon – 6pm; and 6:01 pm – 12:00 midnight in order to establish the busiest to least busiest shopping hours and how this could have an effect upon the cashiers' attention to maintain merchant agreement or store policy pertaining to plastic card transactions. Thirty-one of these thirty-four (34) in store point of sale transactions did not require a pin number to complete the transaction. Three of these transactions did require a pin number, and they were all made using a Visa debit card coded as ending in 3333. Twenty-three of these transactions were made without the need for an electronic signature. All of these twenty-three (23) transactions were under $50.00 each. Each of the eleven (11) transactions that were made with a purchase

amount over $50.00 each did in fact require an electronic signature and it was stated on the receipts of store Chain #1 as 'signature verified.' The total amount of charges applied to a combination of four (4) credit/debit cards utilized was $1,730.48 over a five (5) day period of shopping and observations. $787.64 was spent at store Chain #1 (at fifteen separate stores). $261.01 was spent at store Chain #2 (at eight separate stores). $681.83 was spent at store Chain #3 (at six separate stores). Two MasterCard accounts were used with chip technology and two Visa accounts were used, one debit and one credit, without chip technology and magnetic slide strips and pin numbers. These cards were coded as ending in 1111, and 2222 for the two MasterCard accounts; and, 3333 and 4444 for the two Visa card accounts. The total amount charged at all stores and chains for MasterCard ending in 1111 was $613.06. The total amount charged at all stores and chains for MasterCard ending in 2222 was $897.50. The total amount charged at all stores and chains for Visa debit ending in 3333 was $169.37. Last, the total amount charged at all stores and chains for Visa credit ending in 4444 was $50.55. The times of the day or night were recorded as well as the amount of purchase and the gender and race of the cashier for comparison purposes. Fifteen electronic purchases were made using electronic counters and nineteen non-electronic purchases were made using front registers for comparative purposes of cashier merchants' agreement management. Receipts were saved for documentation but are stored securely in a locked security box.

The following Tables 9-12 are test questions analyzing for absence or presence of capable guardianship, while applying the R.A.T. based upon the accumulative documentations made on each observations report (See Appendix A):

Table 9

Test Question 1 Results for Analyzing Capable Guardianship

Test Question 1 for Analyzing Capable Guardianship: *Did the cashier participant at the POS terminal ask to see the researcher's card in hand being used for payment during any time for any reason while the face-to-face sales transaction occurred?*		
Store Chain # (Coded)	**YES**	**NO**
#1	0:20 **(0%)**	20:20 **(100%)**
#2	0:8 **(0%)**	8:8 **(100%)**
#3	2:6 **(33%)**	4:6 **(67%)**

Table 10

Test Question 2 Results for Analyzing Capable Guardianship

Test Question #2 for Analyzing Capable Guardianship: *Did the cashier specifically check the account numbers or the back of the card to see if the card being used for payment was signed and valid or unsigned and not valid for purchases?*		
Store Chain # (Coded)	**YES**	**NO**
#1	0:20 **(0%)**	20:20 **(100%)**
#2	0:8 **(0%)**	8:8 **(100%)**
#3	0:6 **(0%)**	6:6 **(100%)**

Table 11

Test Question 3 Results for Analyzing Capable Guardianship

Test Question #3 for Analyzing Capable Guardianship: *Did the cashier participant ask the researcher to sign her unsigned card, deemed by Visa and MasterCard alike as "not valid" for purchases, in his or her presence to legitimately authorize it before the face-to-face sales transaction could be processed and completed at the POS terminal?*		
Store Chain # (Coded)	**YES**	**NO**
#1	0:20 **(0%)**	20:20 **(100%)**
#2	0:8 **(0%)**	8:8 **(100%)**
#3	0:6 **(0%)**	6:6 **(100%)**

Table 12

Test Question 4 Results for Analyzing Capable Guardianship

Test Question #4 for Analyzing Capable Guardianship: *Did the cashier participant at the POS terminal ask to see the researcher's government issued photo identification bearing her genuine signature to compare it to the requested signature provided in the presence of the cashier at any time during the face-to-face card in hand in store sales transaction?*		
Store Chain # (Coded)	**YES**	**NO**
#1	0:20 **(0%)**	20:20 **(100%)**
#2	0:8 **(0%)**	8:8 **(100%)**
#3	0:6 **(0%)**	6:6 **(100%)**

Table 13

Results of Accumulative %'s of All Test Questions Combined for Analyzing Capable Guardianship

Store Chain #	TEST QUESTIONS FOR ANALYZING GUARDIANSHIP				
	1	2	3	4	TOTAL COMBINED
#1	0%	0%	0%	0%	0%
#2	0%	0%	0%	0%	0%
#3	33%	0%	0%	0%	8%

This table demonstrates that there was an overall absence of capable guardianship by all three store chains at POS terminals and that their employees are not adhering to Visa and MasterCard policy guidelines outlined by the merchant contracts for acceptance of card payments. Store chain #3's percentage of 33% indicates only that there were two (2) employees that actually took the researcher's credit card in hand before completing the transaction, but it does not explain that those same two employees did so because the researcher could not remember her PIN number being prompted by the electronic processing system and that these two participants, at separate stores and states but within the same store chain, too her card and looked on the back of the card specifically to find the security CVV code to manually input into the system on their side in order to override the need for inputting a PIN number. Both of these

participants had opportunity to notice whether the card was signed and authorized but neither did. So in effect, these two were actually more negligent and there was a greater absence of capable guardianship demonstrated in these numbers that what appears in the table.

Table 14

Variates 1 & 2 in Demographics' Effects on Presence of Capable Guardianship

STORE CHAIN (CODED)	**VARIATES of DEMOGRAPHICS**			
	GENDER		**RACE**	
	MALE	FEMALE	WHITE OR CAUSASIAN	BLACK OR AFRICAN AMERICAN
#1	**0%**	**0%**	**0%**	**0%**
#2	**0%**	**0%**	**0%**	**0%**
#3	**0%**	**0%**	**0%**	**0%**

The 0 %'s represent the percentages of males, and females, both Black and White that demonstrated increased levels of guardianship during accumulative transactions. As this table represents, race nor gender increased levels of capable guardianship and there were no differences observed between male or female participants, nor Black or White participants at POS terminals in each store chain. This table also indicates and overall absence of capable guardianship for both genders and races. In conclusion, the variates of race and gender has had no significant impact on the outcome of this study. Zero percent (0%) of both races and genders

checked the back of the unsigned card being processed for an authorized signature, nor did they require it to be signed nor ask for government issued photo identification.

Table 15

Variates 3, 4, & 5's Effects on Presence of Capable Guardianship
(*Electronic vs. Non-Electronic, Location of POS Terminal inside Store (Front or Back), and Time Segment of Shopping Hours)*

STORE CHAIN (CODED)	**SALES TRANSACTION VARIATES**							
	ELECTRONIC ITEM VS. NON-ELECTRONIC ITEM		**BACK POS TERMINAL VS. FRONT POS TERMINAL**		**TIME SEGMENT (Busy vs. Not Busy)**			
	Electronic	Non-Electronic	Front of store	Back of store	1	2	3	4
#1	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**
#2	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**
#3	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**

This table demonstrates that these three variates: 1) Electronic item vs. non-electronic item, and where the POS terminal was located within the store, 2) Back of store at electronics counter vs. front of the store at checkout near entrance, and 3) Time segment of the day that the transaction occurred and whether the store was experiencing busy shopping hours versus not busy shopping hours, or opening or closing hours, made absolutely no impact on the study or outcome. There was not a higher level of guardianship demonstrated by the participants even when the item was an electronics items or the POS terminal was located in the electronics department. The time segment in which the transaction occurred did not make an impact upon

increasing the presence of guardianship. Overall, there was a generalized absence of capable guardianship demonstrated by all three store chains regardless of all three of these variates. Not one participant checked the back of the credit card to authenticate the researcher's identity prior to processing each transaction. Not one participant required the unsigned card to be signed nor did anyone of the participants request or require government issued photo identification.

Findings on Guardianship Efforts by Participants at POS Terminals

Research Question 1 Findings and Hypothesis Discussed

RQ1: The first research question contains five parts: 1) Will the cashier at the point of sale transaction act as a capable guardian over the face-to-face transaction and act to help prevent identity theft and credit/debit card fraud by taking the card into his or her hand to visually check the back of the credit or debit card to see if it bears an authorized signature by the legal cardholder, or check the account number on the card and compare it to that in the system or receipt in according to the merchant agreement rules as mandated by the Bank Rules and Regulations, Visa and MasterCard? (See Appendices B, C, & D). Variables investigated: 2) Will the variables of non-electronic versus electronic purchase increase levels of capable guardianship? Will there be a difference in the level of capable guardianship if the purchase is made at the back electronic counter POS terminal versus the store's front end POS terminal? 3) Will the higher amount of purchase charges to the card raise levels of guardianship at POS terminals with electronic purchases compared to a low levels of guardianship for small charges to the card? 4) Will the variables of time segment of day or night and business or lack thereof give increase or decrease to the levels of capable guardianship? 5) Will there be a difference of levels of guardianship based upon gender or race of the employee processing the transaction at each POS terminal?

Findings: Table 10 *Test Question #2 for Analyzing Capable Guardianship: Did the cashier specifically check the account numbers or the back of the card to see if the card being used for payment was signed and valid or unsigned and not valid for purchases?,* demonstrates that zero percent (0%) of the participants specifically checked the back of the researcher's unsigned card for an authorized signature validating the card for use. (See page 101 for Table 10). Additionally, the five variates investigated to determine if each in itself or in combination with other variates would raise the level of guardianship and persuade or require the participant employees conducting each transaction at the POS terminals to ask for the researcher's card to specifically check for an authorized signature or compare the account information of numbers on the front of the card to that which was showing in the system. None of these five variates had any impact whatsoever on raising the level of guardianship. The findings conclude that there is an overall absence of capable guardianship at these three store chains POS terminals. (See Table 14, page 104, for variates of demographics of race and gender; see Table 15, page 105, for variates of electronic vs. non-electronic items, time segment of purchase and busy hours or not, and costs of items. See also Tables 11-13, pages 102-103, for test questions determine absence or presence of capable guardianship.)

Hypothesis discussed: Ho1 is validated and proven to be correct based upon the findings that conclude that zero percentage (0%) of the 34 participants at the 28 stores patronized for shopping within the three separate store chains within the Tri-State region checked the back of the researcher's credit or debit card specifically for an authorized signature. Ho1 hypothesized that there would be none that would check the back of her card to see it was unsigned nor require her to sign it, indicating that there is an overall absence of capable guardianship at these

particular retail store chains POS terminals. This validated hypothesis is a critical element to the purpose of this research and the theory behind it.

Research Question 2 Findings and Hypothesis Discussed

RQ2: Will the cashier at the face-to-face transaction at the POS (point-of-sale) terminal require the cardholder and purchaser to sign the back of the unsigned card used for purchase, and will he or she make her show a government issued photo identification for verification of her identity before the transaction is allowed to be processed through, in keeping with merchant agreement rules as mandated by Bank Rules and Regulations, Visa and MasterCard?

Findings: As demonstrated in Table 12 *Test Question #4 for Analyzing Capable Guardianship,* the question was investigated: *Did the cashier participant at the POS terminal ask to see the researcher's government issued photo identification bearing her genuine signature to compare it to the requested signature provided in the presence of the cashier at any time during the face-to-face card in hand in store sales transaction?* The results of all 34 individual transactions conducted by 34 individual participants and accumulated from 28 stores within three national store chains yielded the same zero percent (0%) collectively. (See page 102 for Table 12).

Hypothesis discussed: Ho2 was proven to be correct by this study. Not one employee participant asked to see the researcher's government issued photo identification as mandated by Visa and MasterCard card acceptance guidelines when the credit or debit card is unsigned and not authorized or valid for use. It should be noted that Visa nor MasterCard does not require photo identification for processing signed and authorized cards, but both do so for unsigned cards (See Appendices A, B, & C).

Research Question 3 Findings and Hypothesis Discussed

RQ3: Will the cashier act in lieu of an FDE (Forensic Document Examiner) to investigate by visual comparison the general similarities or differences of handwriting demonstrated on the government issued photo identification bearing a genuine signature of the researcher to that of the unsigned card that should be required to be signed in the presence of the cashier at the POS terminal?

Findings: As demonstrated in Table 9 *Test Question 1 for Analyzing Capable Guardianship: Did the cashier participant at the POS terminal ask to see the researcher's card in hand being used for payment during any time for any reason while the face-to-face sales transaction occurred?*, there were 0% of participants who took the card in hand specifically to check for an authorized signature on the back of the card's signature strip. Subsequently, there were no participants that requested to see government issued photo ID (see Table 12) and have a genuine signature to visualize and used for comparison. None of the participants personally looked at the researcher's signature on either. So zero percent (0%) of the participants attempted to act in lieu of a Forensic Document Examiner (FDE) to determine if the generalized appearance of the signatures being compared were genuine or spurious.

Hypothesis discussed: Therefore, since zero percent (0%) of the participants attempted to act in lieu of a Forensic Document Examiner (FDE) to determine if the generalized appearance of the signatures being compared were genuine or spurious. Ho3 is validated and found to be correct in this study by these participants only. It is important to note that there are other retail stores that do train there their employee participants to attempt to visualize and compare signatures for general similarities or differences but not on the forensic as an FDE.

Research Question 4 Findings and Hypothesis Discussed

RQ4: Will the cashier rely solely upon the electronic capturing device to verify the signature and not personally look at it himself or herself?

Findings: Once again, as demonstrated in Table 9 *Test Question 1 for Analyzing Capable Guardianship: Did the cashier participant at the POS terminal ask to see the researcher's card in hand being used for payment during any time for any reason while the face-to-face sales transaction occurred?*, there were 0% of participants who took the card in hand specifically to check for an authorized signature on the back of the card's signature strip. Subsequently, there were no participants that requested to see government issued photo ID (see Table 12) and have a genuine signature to visualize and used for comparison. None of the participants personally looked at the researcher's signature on either.

Hypothesis discussed: Therefore, Ho4, which hypothesized that the participants would demonstrate accumulative results showing their overall reliance upon technology to process and check for genuine signatures is validated and found to be correct. Table 5 *Itemized List of 34 Purchases, Charges Incurred, and Technology Used for Transaction*, provides an itemized list of the technology that was relied upon for each transaction to be completed. (See pages 92-94)

Research Question 5 Findings and Hypothesis Discussed

RQ5: Will the participant cashier at the POS terminal solely depend upon the EMV chip reader technology newly implemented at the POS terminals equipped with such to "guard" over the identity of the cardholder, even when neither a PIN number nor signature is required nor requested for the transaction to be processed?

Findings: There were comments made by several participants at two separate store chains, #1 and #3, that were included into the additional notes section on the observation reports that the new EMV chip technology made the transaction so safe that they did not need a PIN number for card transactions anymore, when the researcher was asking if she needed to input a PIN number to process the transaction because she did not have one with the particular card being utilized for each of those transactions.

Hypothesis discussed: This observational finding indicates that there is a false expectation by the employee participants of the new EMV chip technology to completely eradicate identity theft related to card fraud, and that it will in essence "guard" over the cardholder's account even without a PIN number. It is reasonable to assume this hypothesis to be somewhat validated based upon those few additional comments made by several participants during those transactions. However, this particular research question and hypothesis would be better investigated and validated by future research involving interviews or surveys completed by employee participants and managers.

CHAPTER 5

DISCUSSIONS

In reviewing the purpose of this research study, the problem of identity theft and plastic card fraud has been increasingly become a national and international problem. The significance of this crime has contributed to rise in white collar criminal activity and has subsequently warranted the increase in technological advances to curtail it, such as electronic signature pads to capture and store digitized signatures, and also the need to implement encrypted chips into American credit/debit cards for security purposes. The areas being investigated by this observational study include two major questions: 1) Are cashiers at point of sale transactions inside the three major department stores that are commonly targeted for fraudulent purchases by plastic card means acting as capable guardians (applying the R.A.T. criminology theory) by checking the backs of credit cards to see if they are authorized with a genuine signature? And 2) If the card is not signed and authorized to make it valid for purchases, are the cashiers asking for or requiring government issued photo identification with a genuine handwritten signature for identification verification purposes and comparison? To investigate these questions, thirty-four individual transactions were made with thirty-four individual cashiers at twenty-eight separate store locations within the three major department store chains, which were coded for privacy. These stores were located within East Tennessee, Virginia, North Carolina, and Georgia. Four separate credit/debit cards were used to make these thirty-four purchases, two of which were MasterCard accounts using chip technology, and two of which were Visa accounts using magnetic slide strips only. The results of this observational study were significant in realizing the absence of capable guardianship at in store point of sale contacts between employees and purchasers. Regardless of time of day transaction took place, or whether or not the store was

busy with other customers waiting in line, or whether the cashier was a female or a male, black or white, no one checked the back of the credit card for an authorized signature. Nor did they follow up according to merchant agreement guidelines and rules of MasterCard and Visa to require a government issued photo identification with a genuine signature for comparison, nor require the purchaser, who was also the primary investigator to sign the back of the card in the white blank strip designated for "AUTHORIZED SIGNATURE" near the statement "NOT VALID UNLESS SIGNED" This negligence is suspected to be in part or whole of improper training or incentives, or unreasonable reliance upon technology—whether it be the electronic signature pads capturing and storing the digitized marks made by purchasers or the new chips that have been encrypted into new credit cards, with or without the use of pin numbers or electronic signatures. This research implies that genuine handwritten signatures are obsolete in store purchases of these specific three large department store chains, without the use of electronic signature pads. The handwritten signature on the backs of the credit or debit cards authorizing the card and making it valid for use is forgotten in practice.

Summary of Findings

The most important findings that have emerged from this observational study are that it does not matter whether the store is busy or not busy, what time of the day or night a consumer shops, or at which of the three major department store chains that were patronized for purchases of electronic items or non-electronic item; or whether the cashier is male or female, Black or White, the cashiers are not aggressively acting in roles of capable guardians to prevent or minimize identity theft and credit/debit card fraud. Nor does it matter if the credit card being utilized has new chip technology or only a magnetic slide stripe, the point of sale transactions are not being guarded capably within these particularly common and popular three chains used for

many electronic purchases. These specific chains were chosen because they are highly targeted by thieves who realize their opportunities for identity theft and credit/debit card fraud because of failure to capably guard point of sale transactions at registers, whether they are electronics counters or front end registers. For reasons yet undisclosed and undiscovered by this qualitative study limited to observations only, cashiers are not effectively guarding sales transactions using plastic payment methods. This could be in part or whole to improper training or incentives to do so, or it could be in part due to apathy or ignorance of merchant agreement rules of MasterCard and/or Visa, which requires an authorized signature on the back of each card issued to make the credit or debit card legally valid for in store use or otherwise. These findings suggest that there is also a strong reliance upon technology for validation of credit or debit cards, and that the new chip technology, as well as the electronically verified signature, has replaced the former style of a legible signature of the legal cardholder and verification of it upon visual inspection and comparison to any government issued photo identification—at least in the minds of the cashiers of these particular store chains. The old-fashioned handwritten signature of an in store purchaser either on the back of their credit card or receipt is all but forgotten it seems. Why is this? The answer to this question is yet to be discovered and warrants future investigation including cashier surveys and manager surveys. The implication is there is an unwarrantedly strong, yet blind reliance upon technology—whether it be a chip in a credit card without a pin for protection, or whether it be an electronic signature that is inconsistently digitized by incongruent strokes or marks when signed in different electronically engineered e-pad systems or even using different signs and symbols to sign it. The conception and perhaps ultimately misconception is that newer methods are better and safer, and that former simpler methods, like that of simply checking the back of a credit or debit card for an authorized signature is no longer necessary. Thus, making it

unnecessary to require any government issued photo identification that would bear the likeness of image of purchaser or the likeness of their genuine handwritten signature. Societal advances beyond common logical reasoning are not truly advances at all, are they? If these technological advances were being used in conjunction with basic preventative measures, such as checking the back of a credit card and requiring a signature and photo identification if not authorized, then they would yield the ultimate capable guardianship potentials. In conclusion, technological guardianship cannot currently be effective without capable human guardianship.

Conclusions

Are the cashiers acting as capable guardians during in store point of sale transactions, in keeping with store policies and merchant agreement contracts between the card issuers of MasterCard and Visa and the legal cardholders of the accounts, in efforts to help prevent and minimize identity theft and credit/debit card fraud? Based upon this qualitative observational research, and these specific findings associated with these thirty-four individual transactions and coherently thirty-four individual cashiers at twenty-eight separate stores within three store chains in a four state region, the answer is 'NO', and one that warrants further investigation. The specific objective of this observational study was to see if each cashier would check the back of the credit/debit card for an authorized signature and require government issued photo identification in the absence of an authorized signature. The conditions involved whether the cashiers were male or female, and how busy or not the store was at the time of purchase. These factors could have an impact on how the transaction was capably guarded or not. For instance, if the store were busy and the lines were long, then the cashier, male or female would be less apt to act as a capable guardian due to job performance pressure and time constraints to keep customers from becoming impatient and irritable. How a male guards the point of sale transaction may

differ from how a female would manage her role as guardian. However, the findings were non-specific to either time of day, busy hours or least busy hours; or whether the cashier acting in role of guardian were male, female, black or white.

Limitations of Thesis Research

This field research was limited strictly to observations made as a credit card payment purchaser in 28 separate large department stores of three commonly targeted chains—all located within the Tri-State region of Eastern Tennessee, Western Virginia, and Northeastern North Carolina and one in Georgia. Therefore, it lacks sufficient quantity for external validity and large generalizability. Additionally, it does not involve guardianship issues related to online identity theft and credit or debit card fraud that is also a major contributor of fraud. The internal validity is weakened in that this study only portrays the observations of those representatives sampled within this specific region. Therefore, the information gathered and coded for this analysis is restricted to observations only and not interviews with individual managers or employees, which may yield additional insight to findings. There is little criminological research done on this specific area of adequate guardianship at point of sale transactions involving in store merchant sales clerk employees or managers and their adherence to the merchant agreement contracts as mandated by Visa, MasterCard and Bank Rules (See Appendix B, C, & D). To date, no criminology research has been reported analyzing why large scale identity theft in credit and debit card fraud occurs at specific large department store chains or why they are strongly considered as suitable targets by motivated fraud offenders.

Recommendations

Recommendations based upon this observational study include training of managers and employees as to the necessity of basic preventative measures of checking for signatures and asking for photo identification when there is none, in common sense efforts to prevent identity theft and plastic card fraud. There is also an indication that sole reliance upon technology without these basic preventative measures leads to opportunities for identity theft and credit/debit card fraud to continue on aggressively as criminal minds search for system loopholes. In comparing what has been discovered in data collection, data analysis, and discussion, this study reveals the need for educating cashiers to be better equipped at capable guardianship at point of sale contacts with purchasers and potential identity thieves using credit/ debit card fraud. This study reveals that cashiers are not acting as capable guardians in keeping with merchant agreement obligations with MasterCard and Visa and simply checking the backs of credit or debit cards to see if there is an authorized signature, nor asking for government issued photo identification if there is not. Inadvertently, this study shows that handwritten signatures are a thing of the past at point of sale transactions and are primarily used only on electronic pads to make a mark—any mark. If these store chains and others were to couple the use of technology with aggressive preventative practices of checking for handwritten signatures and requiring photo identification for visual comparisons of the person and the person's handwritten signatures, and do so consistently across all store chains and businesses, then in store fraudulent purchases would be expected to diminish. Training cashiers to become adequate in capable human guardianship would provide most promising results in diminishing in store fraud occurring repeatedly at targeted store chains. The Routine Activities Theory is the most plausible to be applied to these daily transactions within businesses and should be carefully

analyzed and utilized by security within each department store chain to develop the best overall plan for prevention of fraud.

Future Research

This study raises awareness and demonstrates the need for future research regarding the consumer habits of signing electronic signature pads and with what marks to determine the true value and usefulness of this technology in preventing or identifying identity theft and non-genuine signatures of purchasers. Future research is also indicated in determining the usefulness of chip technology without the use of pin numbers, and only chip and electronic signatures. While there is capacity to store electronic signatures and recall them on a need to know basis, the validity of the same may never come into question if there is no need to know and does not serve as a deterrent nor preventative of crime. It is only somewhat useful if the legal cardholder and purchaser signs consistently with the same marks, or fluidity of digitized signature. A cross study of international practices of other countries using both chip and pin technology, and other technology such as retina identification, etc. coupled with visual inspection of authorized signatures and photo identification with genuine signatures is imperative to gain a full comprehensive perspective on the practices that are most beneficial in curbing identity theft and credit/debit card fraud, in our American society, and international community.

REFERENCES

Allison, S.F.H., Schuck, A.M., & Lersch, K.M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates and victim/offender characteristics. *Journal of Criminal Justice, 33*, 19-29. doi: 10.1016/j.jcrimjus.2004.10.007

Anderson, K.B., Durbin, E., & Salinger, M.A. (2008). Identity Theft. *Journal of Economic Perspectives, 22*(2), 171-192.

Authentication. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-authentication.php#ixzz44QiYiY5C

Authorization. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-authorization.php#ixzz44Qk0QHry

Authorized Transaction. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-authorized-transaction.php#ixzz44Qm0vvcn

Baldwin, F.N., Jr. (2002). Organized crime, terrorism and money laundering in the Americas. *Florida Journal of International Law Documents, 15*(3), 8. Retrieved from http://lexisnexis.com/Inacui2api/deliver/PrintDoc.do?fromCar…2/24/2014.

Bank card merchant rules and regulations. (2004). Retrieved from www.finance.umich.edu/system/files/ccRulesRegs_Jan2004.doc

Barker, K.J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: Awareness and prevention. *Journal of Financial Crime, 15*(4), 398-410. doi: 10.1108/13590810907236

Bernburg, J.G., & Thorlindsson, T. (2001, September). Routine activities in social context: A closer look at the role of opportunity in deviant behavior. *Justice Quarterly (JQ), 18*(3), 543-553.

Boetig, B.P. (2006, June). The routine activity theory: A model for addressing specific crime issues. *FBI Law Enforcement Bulletin, 75*(6), 12-99.

Bolton, R.J., & Hand, D.J. (2002, August). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235-249. Retrieved from http://www.jstor.org/stable/3182781

Bossler, A. M., & Holt, (2009, January-June). Online activities, guardianship, and malware Infection: An examination of routine activities theory. *International Journal of Cyber Criminology (IJCC), 3*(1), 400-420.

Bossler, A.M., & Thomas, J.H. (2009, January/June). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology (IJCC), 3*(1), 400-420.

Budhram, T. (2012, June). Lost, stolen or skimmed. *SA Crime Quarterly, 40*, 31-37.

Choi, K. (2008, January/June). Computer crime victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology (IJCC), 2*(1), 308-333.

Card Present. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-cardpresent-transactions.php#ixzz44QnAw7br

Card Present Fraud. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-cardpresent-fraud.php#ixzz44QofEZmz

Card Present (CP) Transactions. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-cardpresent-cp-transactions.php#ixzz44QoC8hcf

Chargebacks. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-chargeback.php#ixzz44SAkqmni
Chip card ATM 'shimmer' found in Mexico. (August 2015). Retrieved from http://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/
Chip Enabled Terminal. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-chipenabled-terminal.php#ixzz44QqkDETU
Chip and Pin Cards. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-chipandpin-cards.php#ixzz44Qq5QVYj
Chip and Signature. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-chip-and-signature.php#ixzz44QphZ5Gf
Choi, K. (2008, January/June). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology (IJCC), 2*(1), 308-333.
Choo, K.K. R. (2011). The cyber treat landscape: Challenges and future research directions. *Computers and Security, 30*, 720-731. doi: 10.1016/j.cose.2011.08.004
Cloning. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-cloning.php#ixzz44S0D53cb
Copes, H., Vieraitis, L., & Jochum, J.M. (2007, November). Bridging the gap between research and practice: How neutralization theory can inform Reid interrogations of identity thieves. *Journal of Criminal Justice Education, 18*(3), 444-459. doi: 10.1080/10511250701705404.
Copes, H., & Vieraitis, L. (2009, June). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy, 8*(2), 237-262.
Credit Card. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-credit-card.php#ixzz44S4OOvBO
Credit Card Number. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-credit-card-number.php#ixzz44S5qBZh2
CVV. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-cvv.php#ixzz44S3g5IgE
Davenport, T. H. (2006, January). Competing on analytics. *Harvard Business Review: Decision Making,* 1-10.
Debit Card. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-debit-card.php#ixzz44S420PMf
Doig, A., Johnson, S., & Levi, M. (2001). New public management, old populism and the policing of fraud. *Public Policy and Administration, 16*(91), 91-113. doi: 10.1177/095207670101600106
Duman, E., & Ozcelik, M.H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications, 38*, 13057-13063.
Electronic measures, procedures impact credit card fraud levels. (2000, April). *Security, 37*(4), 82.
EMV Card. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-emv-card.php#ixzz44QhTECYI
EMV Liability Shift. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-emv-liability-shift.php#ixzz44S1IjHAi
Encryption. (n.d.) Retrieved from

http://www.creditcards.com/glossary/term-encryption.php#ixzz44S168ShK
Fahmy, D. (2010). Credit card crooks like to shop at Best Buy, Target, and Amazon. Retrieved from http://abcnews.go.com/Business/credit-card-theft-crooks-shop-best-buy-target/print?id=993
False Positives. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-encryption.php#ixzz44S168ShK
Four risky places to swipe your debit card. (2014). Retrieved from http://www.bankrate.com/system/util/print.aspx?p=/finance/checking/risky-places February 26, 2010.
Fraud Alert. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-fraud-alert.php#ixzz44QyFpjPh
Fraudulent Transaction. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-fraudulent-transaction.php#ixzz44Qxh1vKy
Fraudulent User. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-fraudulent-user.php#ixzz44QxHQ2vA
Free, C. & Murphy, P.R. (2014). The ties that bind: The decision to co-offend in fraud. *Contemporary Accounting Research.* Advance online publication. doi: 10.1111/1911-3846.12063
Fullerton, R.A, & Punj, G. (2004). Repercussions of promoting an ideology of consumption: Consumer misbehavior. *Journal of Business Research, 57*, 1239-1249. doi: 101016/ S0148-2963(02)00455-1
Groff, E.R. (2008). Adding the temporal and spatial aspects of routine activities: A further Test of routine activity theory. *Security Journal, 21*, 95-116. doi: 10.1057/palgrave.sj. 8350070
Harrell, E. (September 2015). *Victims of Identity Theft, 2014* (NCJ 248991). U.S. Department of Justice, Office of Justice Programs, *Bureau of Justice Statistics*. Retrieved from www.bjs.gov/content/pub/press/vit14pr.cfm
Harrell, E. & Langton, L. (December 2013). *Victims of Identity Theft, 2012*, (NCJ 243779). U.S. Department of Justice, Office of Justice Programs, *Bureau of Justice Statistics*. Retrieved from www.bjs.gov/content/pub/pdf/vit12.pdf
Hechter, M., & Kanazawa, S. (1997). Sociological Rational Choice Theory. *Annual Review of Sociology, 23*, 191-214.
Holtfreter, K., Reisig, M.D., & Pratt, T.C. (2008). Low self-control, routine activities, and fraud Victimization. *Criminology, 46*(1), 189-220.
Identity Theft. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-identity-theft.php#ixzz44QmUIwoB
Important information about unsigned credit cards: MasterCard rules and security procedures require that credit cards must be signed by the cardholder in order to be accepted for payment. (n.d.). Retrieved from https://www.mastercard.com/us/merchant/pdf/Unsigned_Credit_Cards-(Global).pdf
Kleemans, E.R., Soudijn, M.R.J., & Weenink, A.W. (2012). Organized crime, situational crime prevention and routine activity theory. *Trends in Organized Crime, 15*, 87-92. doi: 10.1007/s12117-012-9173-1
Krebs, B. (2015). Definition of 'shimming.' Retrieved from http://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/

Lee, B., Hyungjun, C., Chae, M., & Seonyoung, S. (2010). Empirical analysis of online auction fraud: Credit card phantom transactions. *Expert Systems with Applications, 37*, 2991-2999.

Lilly, J.R., Cullen, F.T., & Ball, R.A. (2011). Chapter 13: Choosing crime in everyday life. 328-350. *Criminological Theory: context and consequences, 5th Ed*., California: Sage Publications.

LoPucki, L.M. (2001-2002). Human identification theory and the identity theft problem. *Texas Law Review, 80*, 89-136. Retrieved from http://ssrn.com/abstract=263213

Magnetic Stripe. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-magnetic-stripe.php#ixzz44QtvgUn4

MasterCard Card. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-mastercard-card.php#ixzz44QrpyHgu

Masuda, Barry. (1997). Credit card fraud prevention: A successful retail strategy. 121-134. Report prepared for Tops Appliance City, Inc., New Jersey: New York.

Merchant Agreement. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-mastercard-card.php#ixzz44QrpyHgu

Papadopoulos, A., & Brooks, G. (2011). The investigation of credit card fraud in Cyprus: Reviewing police "effectiveness." *Journal of Financial Crime, 18*(3), 222-234. doi: 10.1108/13590791111147442

Phishing. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-phishing.php#ixzz44S7vDWMF

PIN. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-pin-personal-identification-number.php#ixzz44RzCrKKh

POS. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-point-of-sale-pos.php#ixzz44QtGKEAg

Prabowo, H.Y. (2011). Building our defense against credit card fraud: A strategic view. *Journal of Money Laundering Control, 14*(4), 371-386. doi: 10.1108/13685201111173848

Pratt, T. C., Holtfreter, K., & Reisig, M.D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 268-296. doi: 10.1177/0022427810365903

RAM Scraping Attack. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-ram-scraping-attack.php#ixzz44S8PXDWn

Reyns, B.W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Safety, 12*(2), 99-118. Retrieved from http://www.palgrave-journals.com/cpcs/

RFID. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-rfid.php#ixzz44S9ACfhK

Rowen, M.J., Beatson, R., & Kelty, M.A. (September 29, 2011). Reduction of fraud through the use of automated centralized signature/sign verification combined with credit and fraud scoring during real-time payment card authorization processes. United States Patent Application Publication. Pub. No.: US 2011/0238510 A1.

Sampson, R., Eck, J.E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal, 23* (1), 37-51. doi: 10.1057/sj.2009.17:published online 12 October 2009

Security Code. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-security-code.php#ixzz44S1uatHH
17.9 Million U.S. Residents Experienced Identity Theft in 2014. *Bureau of Justice Statistics*, Retrieved from https://www.bjs.gov/content/pub/press/vit14pr.cfm#
Signature Strip. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-signature-strip.php#ixzz44Ql5SHyy
Skimmer. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-skimmer.php#ixzz44Qyf0tHp
Skimming. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-skimming.php#ixzz44QywLvZ4
Slotter, K. (1997, June). Plastic payments: Trends in credit card fraud. *FBI Law Enforcement Bulletin, 66*(6), 1-7.
Smishing. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-smishing.php#ixzz44S2mgBiJ
Smith, M. (2007, May). Fraud prevention takes visa. *Optimize.* 37.
Synthetic Identity Theft. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-synthetic-identity-theft.php#ixzz44S51Xi8K
Transaction. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-transaction.php#ixzz44QsQ85Bz
Tillyer, M.S. & Eck, J.E. (2011). Getting a handle on crime: A further extension of routine activities theory. *Security Journal*, 24(2), 179-193. doi: 10.1057/s.2010.2; published online 7 June 2010
Tunley, M. (2011). Uncovering the iceberg: Mandating the measurement of fraud in the United Kingdom. *International Journal of Law, Crime and Justice, 39*,190-203.
Vaughn, D. (1998). Rational choice, situated action, and the social control of organizations.
Law & Society Review, 32(1), 23-61.
Two-Factor Authentication. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-twofactor-authentication.php#ixzz44S9g7pVc
U.S. Department of Justice. (November 2, 2015). Identity theft-criminal fraud. Retrieved from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
User Authentication. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-user-authentication.php#ixzz44QsiX2Z9
Vaughan, D. (1998). Rational choice, situated action, and the social control of organizations. *Law & Society Review, 32*(1), 23-61.
Visa. (October 19, 2015). Card acceptance guidelines for Visa merchants, 32-33. Retrieved from https://usa.visa.com/dam/VCOM/download/merchants/card-acceptance-guidelines-for-merchants.pdf
Visa Card. (n.d.) Retrieved from http://www.creditcards.com/glossary/term-visa-card.php#ixzz44QrNAjv0
What is EMV Chip Card Technology? (n.d.). Retrieved from https://www.level2kernel.com/emv-guide.html
White, M.D., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to Effective prevention and control efforts. *Criminal Justice Policy Review, 19*(3*),* 3-16. doi: 10.1177/0887403407306297

Willacker, G. (February 19, 2014). Accepting Unsigned Payment Cards. *PCI DSS News* and *Information.* Retrieved from treasuryinstitutepcidss.blogspot.com/2014/02/accepting-unsigned-payment-cards.html

APPENDICES

Appendix A:

OBSERVATIONS REPORT

Store Chain: _____ (Coded 1, 2 or 3)
Store Location: _____ (TN, NC, VA, or GA)
Time Category: _____ (Coded 1, 2, 3 or 4)
Exact Time of Transaction and Observations: _____ (Not coded)
Gender of Cashier at POS Terminal: _____ (Male or Female)
Race of Cashier at POS Terminal: _____ (White or Black)
Counter: _____ (Back of Store Electronics or Front of Store)
Classification of Item: _____ (Electronic or Non-Electronic)
Item Purchased: _____
Cost of Purchase: _____
Amount Charged to Card: _____
Type of Card Used for Payment: _____ (MasterCard/VISA)
Security Features of Card Used: _____
(EMV + Magnetic Strip vs. Magnetic Strip Only)
Specific Card Used for Payment: _____
(1:4 Choices, Coded as ending in: 1111, 2222, 3333, 4444)
Did cashier check back of card for authorized signature? _____ (Yes/No)
Did cashier note that card was not signed? _____ (Yes/No)
Did cashier ask for it to be signed in the cashier's presence? _____ (Yes/No)
Did the cashier ask to see government issued photo identification? _____(Yes/No)
Did the purchase require an electronic signature? _____(Yes/No)
Did the purchase require a pin number? _____ (Yes/No)
Additional:_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Appendix B:

Bank Card Rules and Regulations

BANK CARD MERCHANT RULES AND REGULATIONS January 2004

-1 -

Since you (hereinafter "Merchant") have either entered into a Bank Card Merchant Agreement and/or related agreements (collectively referred to herein as "Bank Card Merchant Agreement") with Fifth Third Bank (collectively referred to herein as "FTB") or receive Visa and/or MasterCard acquiring and/or related services from FTB, Merchant agrees to comply with and be bound by these Bank Card Merchant Rules and Regulations ("Bank Rules"). These Bank Rules may be altered or amended from time to time at FTB's sole discretion and without notice. Merchant also agrees to comply with and be bound by the Visa U.S.A Inc. By-Laws and Operating Regulations, the Visa International Operating Regulations and any other rules, policies or requirements of Visa or any of its subsidiaries or affiliates (collectively "Visa Rules") and the MasterCard International Inc. By-Laws and Operating Regulations and any other rules, policies or requirements of MasterCard or any of its subsidiaries or affiliates (collectively "MasterCard Rules"), any of which may be altered or amended from time to time and without notice, which are referenced herein and hereby incorporated into these Bank Rules as if fully rewritten herein. Except for those terms specifically defined herein, all capitalized terms used herein shall have the same meanings as ascribed to them in the Bank Card Merchant Agreement. Merchant may now, or in the future, participate in one or more other card programs which are supported by FTB in accordance with its standards ("Other Programs"), including but not limited to Voyager and Wright Express, and may receive services related to these Other Programs from FTB. In the event that Merchant participates in any such Other Programs, Merchant agrees to comply with and be bound by the Other Programs Bank Rules published by FTB from time to time, as well as any operating rules or regulations or any other rules, policies or requirements of the applicable Other Program(s) ("Other Program Rules"). Before Merchant participates in any Other Program, Merchant agrees that it shall request from FTB in writing a copy of the Other Programs Bank Rules. The Bank Card Merchant Agreement, Visa Rules, MasterCard Rules, Other Program Rules, Other Program Bank Rules and these Bank Rules are intended to be and shall be construed as consistent parts of a whole as applied to the applicable product type. In the event of a direct conflict between the Bank Card Merchant Agreement or the Bank Rules and the Visa Rules or the MasterCard Rules, the Visa Rules and MasterCard Rules shall control; provided, however, Merchant acknowledges and agrees that all agreements with respect to the obligations and liability of FTB are specified in the Bank Card Merchant Agreement and the Bank Card Merchant Agreement shall control on such subjects notwithstanding anything in the Bank Rules, Visa Rules, MasterCard Rules, Other Programs Bank Rules, and/or the Other Program Rules.

A. Honoring of Cards

1. The Merchant shall promptly and without discrimination honor all valid Cards within the appropriate categories of acceptance when properly presented as payment from Cardholders for the purchase of goods and/or services. The Merchant shall maintain a policy that shall not discriminate among customers seeking to make purchases through use of a valid Card. An unreadable magnetic stripe, in and of itself, does not deem a Card invalid.

2. The Merchant shall not establish minimum or maximum sales transaction amounts as a condition for honoring a Card.

3. The Merchant shall not impose any surcharge on sales transactions.

4. Any purchase price advertised or otherwise disclosed by the Merchant must be the price available when payment is made with a Card.

5. Any tax required to be collected by the Merchant must be included in the total transaction amount and not collected separately in cash.

6. The Merchant shall validate all cards by ensuring the signature on the back of the Card matches the signature on the transaction receipt.

7. The Merchant shall not accept any Card having two signatures on the signature panel located on the back of the Card.

8. The Merchant shall not impose a requirement on Cardholders to provide any personal information, such as a (i) home or business telephone number, (ii) home or business address, (iii) driver's license number, (iv) photocopy of a driver's license or (v) photocopy of the Card, as a condition for honoring a Card unless such information is required (a) for mail order, telephone order, or electronic commerce transactions; (b) the transaction amount exceeds a pre-determined dollar limit set by FTB; or (c) the information is required by the Card issuer. Except for the specific circumstances cited above, the Merchant shall not refuse to complete a sales transaction solely because a Cardholder who has complied with all of the conditions for presentment of a Card at the point-of-sale refuses to provide such additional personal information.

9. A Merchant must not refuse to complete an electronic commerce transaction solely because the Cardholder does not have a digital certificate or other secured protocol.

10. The Merchant shall not require a Cardholder, as a condition for honoring a Card, to sign a statement that in any way states or implies that the Cardholder waives any rights to dispute the transaction with the Card issuer or otherwise.

B. Use of Service Marks

1. The Merchant shall adequately display, in accordance with the Visa and MasterCard Rules, the Visa and MasterCard service marks, as applicable, at points of interaction and on promotional materials to indicate which Cards will be honored at the Merchant's place of business. At a minimum, the Visa and MasterCard service marks should be on display near the entrance of the Merchant's place of business and must not be less prominent than other service marks that the Merchant has on display (e.g., American Express, Discover).

2. The Merchant may use the Visa and MasterCard wordmark on promotional, printed, or broadcast materials only to indicate that Cards are accepted for payment and shall not indicate, either directly or indirectly, that Visa and MasterCard endorse any goods and/or services.

3. A merchant web site must display the Visa and MasterCard Marks in full color to

indicate card acceptance. The Visa and MasterCard wordmark should be used to indicate acceptance of cards when a visual representation of the marks is not possible at the merchant web site.

4. The Merchant may not refer to Visa and MasterCard in stating eligibility for its products, services or membership.

C. Authorization

1. The Merchant shall obtain authorization for each sales transaction for the total amount of such transaction. For sales transactions not processed through an electronic terminal, the Merchant shall type or print legibly on the sales draft the authorization approval code evidencing the authorization so obtained.

2. A Merchant must only deposit transaction receipts that directly result from Cardholder transactions with that Merchant. A Merchant must not deposit a transaction receipt that it knows or should have known to be either fraudulent or not authorized by the Cardholder

3. A Merchant is responsible for its employees' actions while in its employ.

4. The Merchant's designated authorization center, or at FTB's option the authorization center designated by FTB (hereafter referred to as "Designated Authorization Center"), provides such Merchant approval or denial for sales transactions for specific dollar amounts. The Designated Authorization Center may also provide the Merchant with assistance in the following circumstances.

a. When a sales transaction involves use of a Card and the total amount of the transaction is in excess of the then current and applicable floor limit, if any, in the Bank Card Merchant Agreement or if a zero floor limit is applicable to such transaction or if there is no mention of a floor limit in the Bank Card Merchant Agreement.

b. When a sales transaction is completed in partial payment of a single purchase, authorization is required for the amount segment(s) of the purchase effected with the Card, regardless of the Merchant's floor limit.

c. When a sales transaction is a mail order or telephone order transaction.

d. When a sales transaction, other than mail order or telephone order, involves (i) a handwritten sales draft which does not contain the imprint of the Merchant plate or the Card, (ii) a Cardholder who is present but without the Card, (iii) a sales draft which is not signed by a Cardholder, (iv) an unsigned Card, (v) suspicious or unusual circumstances or (vi) an expired Card. When requesting authorization in such circumstances, the Merchant must advise the Designated Authorization Center of the specific reason(s) authorization is requested.

(1) If the signature panel on the Card is blank, in addition to requesting authorization, the Merchant must do all of the following.
(a) Review positive identification to determine that the user of the Card is the Cardholder. Such identification must consist of a current, official government identification document (e.g., passport, driver's license) that bears the Cardholder's signature. Such identification, including any serial number, social security number, or driver's license number and expiration date, must be indicated on the sales draft

(b) Require the Cardholder to sign the signature panel of the Card prior to completing the transaction.

(2) If a sales transaction involves suspicious or unusual circumstances, then the Merchant shall call the Designated Authorization Center and request a "Code 10" authorization.

5. An authorization code only indicates the availability of a Cardholder's credit as of the time the authorization is obtained. An authorization is no guarantee that the person presenting the Card is the rightful Cardholder or that the transaction will not be charged back to the Merchant.
6. In the event FTB for whatever reason is unable to obtain, or due to system delays chooses not to wait to obtain, authorization from the Cardholder's financial institution, Visa or MasterCard, FTB may at its option "stand-in" for such entities and authorize the sales draft or sales transaction based on criteria established by FTB, and Merchant remains responsible for such sales draft or sales transaction in accordance with the Bank Card Merchant Agreement.
7. If a sales transaction is not authorized, the Merchant must not complete the sale. A declined sales transaction is originated from the bank that issued the Card. The fact that a sales transaction was declined should not be interpreted as a reflection of the Cardholder's credit worthiness. If the Cardholder has any questions concerning the authorization, instruct such Cardholder to call the bank that issued the Card.

D. Verification and Recovery of Cards

1. If a transaction is not authorized, the Merchant must not complete the sale, and, if instructed by the Designated Authorization Center to pick-up the Card, the Merchant should do so by reasonable and peaceful means, notify the Designated Authorization Center when the Card has been recovered, and ask for further instructions.

2. The Merchant shall use reasonable and peaceful means to recover any Card if (i) the account number thereon is listed on any Combined Warning Bulletin, (ii) the printed four digits above the embossed account number do not match the first four digits of the account number, (iii) the Merchant is advised to retain it or (iv) the Merchant has reasonable grounds to believe such Card is counterfeit, fraudulent or stolen. The Merchant shall also note the physical description of the

Appendix C:

Visa Rules for Unsigned Cards

Cardholder Verification and Identification

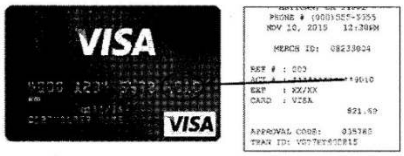
The final step in the card acceptance process for transactions is to verify the cardholder's signature, PIN or other methods as required in the Visa Rules. Visa supports a range of cardholder verification methods including signature, PIN, and PIN-less methods such as CDCVM (Consumer Device Cardholder Verification Method).

1. **Signature** – Verify that the signature on the Card matches the signature on the Transaction Receipt and on any identification required and presented
2. **PIN** – Verification using an acceptance device with electronic capability accepts a cardholder's PIN rather than a signature. The merchant must not ask the cardholder to reveal the PIN.
3. **CDCVM** – a verification that is performed on the consumer's payment device, independent from the reader (such as a mobile phone).

Checking Signatures

All attended devices must support signature cardholder verification. Depending on the Visa card product and point-of-sale terminal processing system, the customer should be in full view when signing the receipt or point-of-sale terminal signature window display. If possible, check the two signatures closely for any obvious inconsistencies in spelling or handwriting.

- For magnetic-stripe card transactions, match the name and last four digits of the account number on the card to those printed on the receipt.



- When a signature has been obtained, match the signature on the back of the card to the signature on the receipt. The first initial and spelling of the surname must match.

For suspicious or non-matching signatures, adhere to your merchant store procedures and respond accordingly.

When a Signature Line is Not Present

When a transaction is PIN or CDCVM verified, Visa's best practice is **not** to print a signature line on the receipt. Merchants need to be aware that they should not request a signature from the cardholder when a signature line is not present on the receipt.

Unsigned Cards

While checking card security features, you should also make sure that the card is signed. An unsigned card is considered invalid and should not be accepted. If a customer gives you an unsigned card, the following steps must be taken:

- **Check the cardholder's ID.** Ask the cardholder for some form of official government identification, such as a driver's license or passport. Where permissible by law, the ID serial number and expiration date should be written on the sales receipt before you complete the transaction.
- **Ask the customer to sign the card.** The card should be signed within your full view, and the signature checked against the customer's signature on the ID. A refusal to sign means the card is still invalid and cannot be accepted.
- **Ask the customer for a different signed Visa card.**

The words "Not Valid Without Signature" appear above, below, or beside the signature panel on all Visa cards.

"See ID"

Some customers write "See ID" or "Ask for ID" in the signature panel, thinking that this is a deterrent against fraud or forgery; that is, if their signature is not on the card, a fraudster will not be able to forge it. In reality, criminals often don't take the time to practice signatures. They use cards as quickly as possible after a theft and prior to the accounts being blocked. They are actually counting on you not to look at the back of the card and compare signatures; they may even have access to counterfeit identification with a signature in their own handwriting.

In this situation, follow recommended steps listed above under Unsigned Cards.

Requesting Cardholder ID

When should you ask a cardholder for an official government ID? Although Visa Rules do not preclude merchants from asking for cardholder ID except in the specific circumstances discussed in this guide, merchants cannot make an ID a condition of acceptance. Therefore, merchants cannot as part of their regular card acceptance procedures refuse to complete a purchase transaction because a cardholder refuses to provide ID. It is important that merchants understand that the requesting of a cardholder ID does not change the merchant's liability for chargebacks. However, it can slow down a sale and annoy the customer. In some cases, it may even deter the use of the Visa card and result in the loss of a potential sale. Visa believes merchants should not ask for ID as part of their regular card acceptance procedures. Laws in several countries also make it illegal for merchants to write a cardholder's personal information, such as an address or phone number, on a sales receipt. If you are suspicious, follow recommended steps listed above under *Unsigned Cards*.

Appendix D:

MasterCard Rules Unsigned Card

MasterCard
Worldwide

IMPORTANT INFORMATION ABOUT UNSIGNED CREDIT CARDS

MasterCard rules and security procedures require that credit cards must be signed by the cardholder in order to be accepted for payment

If an unsigned card is presented, the merchant must:

- Obtain usual authorization for the transaction;
- Ask the customer to provide confirming identification; and
- Require the cardholder to sign the card. The merchant must not complete the transaction if the cardholder refuses to sign the back of their card.

What if the card says "Ask for Photo I.D." in the signature space?

- The transaction cannot be processed unless the cardholder's signature appears in the signature space.
- As noted on the cards, they are "not valid unless signed."

Why do cards need to be signed?

- The signature on the back of the card is one of a multi-layered set of security protections in place for cardholders and merchants. The presentation of a signed card allows the merchant to verify the cardholder's identification by comparing the signature on the card to that on the sales receipt.

GUARD YOUR CARD

Other tips for cardholders:

- Never leave your purse or wallet unattended. Keep your personal data and information guarded at all times.
- Sign your credit card as soon as you receive it. Call your card issuer if a new or reissued card does not arrive when expected.
- Never throw away receipts or statements in a public trash container, and be sure to destroy or shred the areas where the account number is visible.
- Make a note of when your financial statements arrive each month. If your statements stop arriving, contact your bank. Read through your monthly statements carefully.
- Do not provide your account number over the phone unless you are positive the call is legitimate. Never provide your credit card number over the phone if you did not initiate the call.
- Keep a list of your credit card accounts, bank accounts, and financial institutions telephone numbers in a secure place so you can quickly call the card issuer(s) to inform them about missing or stolen cards.
- Memorize your passwords and personal identification numbers (PINs) so you do not have to write them down.
- When making a purchase, keep your card in view at all times. Retrieve the card as soon as the transaction is complete and make sure it is yours.
- Don't carry your social insurance card, birth certificate, or passport with you unless it's absolutely necessary. These items can be used for identity theft.
- Be aware of your surroundings. Make sure no one is watching you input your PIN.

Retrieved from https://www.mastercard.com/us/merchant/pdf/Unsigned_Credit_Cards-(Global).pdf

VITA

BELINDA R. WILSON

Personal Data:	Date of Birth: February 24, 1966 Place of Birth: Fort Polk, Louisiana Marital Status: Divorced
Education:	Master of Arts/ Criminal Justice and Criminology, East Tennessee State University, Johnson City, Tennessee. May 2016. Certificate in Forensic Document Examination, East Tennessee State University, Johnson City, Tennessee, August 2013. Bachelor of Arts/ English, Minor/International Studies with Asian Concentration, East Tennessee State University, Johnson City, Tennessee, August 2012. Associate of Arts/English, May 2007, Associate of Science/General, May 2006, Walter State Community College, Greeneville, Tennessee.
Professional Experience:	Forensic Document Examiner Apprentice for Dr. Larry Miller, present Graduate Assistant, Interlibrary Loan Research Assistant, 2013-2015, U.S. Census Bureau, Crew Leader, Greene County, Tennessee, 2000 & 2010, U.S. Congress Intern, International Legislation, for Senator Mary Landrieu, 2008, Private Math and Science Tutor since 2004, Homemaker and Mother since 1986
Honors and Awards:	Alpha Phi Sigma, Criminal Justice Honor Society, inducted 2013, Phi Kappa Phi, International Honor Society, 2013 as Graduate Student, Phi Kappa Phi, International Honor Society, since 2007 as Undergraduate, Phi Sigma Pi National Honor Fraternity, since 2010, TN Board of Regents Scholarship $10,000 The Washington Center, D.C., 2008 Most Outstanding Student Award, Walter State Community College, 2006

Associations:	Greene County Skills, District Council Board Member, since 2015.
	Student Member of: N.A.D.E. (National Association of Document Examiners), A.F.D.E. (Association of Forensic Document Examiners), A.B.F.D.E. (American Board of Forensic Document Examiners)
Presentations:	"Exploding Dye Packs in Currency" – N.A.D.E. Convention, Nashville, TN, April, 2015.
	"Identity Card Theft" – Money Smart @ ETSU 2016 East Tennessee State University, Johnson City, TN, April 21, 2016.
	"The Forgotten Signature" – AFDE Symposium, Myrtle Beach, SC, October 2016.