AN EVALUATION OF A BIOMETRIC ENABLED CREDIT CARD FOR PROVIDING HIGH AUTHENTICITY IDENTITY PROOFING DURING THE TRANSACTION AUTHENTICATION PROCESS

A Dissertation

Presented to

The College of Graduate and Professional Studies

College of Technology

Indiana State University

Terre Haute, Indiana

In Partial Fulfillment of the

Requirements for the Degree

Doctor of Philosophy

by

Laura F. Poe

May 2019

Keywords: Biometrics; Identity Proofing; Fraud Prevention; User Authentication, Technology Management

Laura F. Poe

110 Seaton Drive
Colonial Heights, VA 23834

Education

B.S., Information Systems, Virginia Commonwealth University, Richmond, Virginia, 1999
B.S., Accounting, Virginia Commonwealth University, Richmond, Virginia, 1999
MS, Business, Information Systems, Virginia Commonwealth University, Richmond, Virginia, 2002
MA, Theological Studies, Liberty University, Lynchburg, Virginia 2010
PhD., Technology Management, Indiana State University, Terre Haute, Indiana, 2018

Professional Experience

DigiTek LLC	CEO & Principal Consultant	2017-present
Capital One	Manager, Cyber Security	2010-2017
Dominion Resources	Business Systems Analyst	2008-2010
Philip Morris USA / Altria	SAP Configuration Analyst	1998-2008

Academic Experience

University of Richmond	Adjunct Faculty, School of Professional and Continuing Studies	2018-present
Liberty University Lynchburg, VA	Adjunct Faculty, Business – Information Systems	2018-present
John Tyler Community College Chester, VA	Adjunct Instructor, Computer Information System	2010-2011
Strayer University Glen Allen, VA	Adjunct Professor, Computer Information Systems	2004-2005

Presentations & Publications

2016, Biometric Applications for Credit Card Fraud Prevention, International Conference for Technology Management, Chicago, IL
2018, Biometrics as Identity Proof, Information Security Conference, Richmond, VA

Certifications

Certified Cloud Security Professional (CCSP), Certified Scrum Master (CSM), Certified Scrum Product Owner (CSPO), SAP Finance (FI), Controlling (CO), Sales & Distribution (SD), (Solution Manager) SM

COMMITTEE MEMBERS

Committee Chair: Dr. Elaine D. Seeman, PhD

Chair and Professor, Department of Management Information Systems

East Carolina University

Committee Member: Dr. Robert A. Chin, PhD

Professor, Department of Technology Systems

East Carolina University

Committee Member: Dr. Xiaolong Li, PhD

Associate Professor, Department of Electronics and Computer Engineering Technology

Indiana State University

ABSTRACT

Credit card fraud has continued to grow despite efforts to protect financial data from data breaches of financial institutions. Data breaches of financial transactional records over the past decade have impacted millions of U.S. consumers, resulting in decreased consumer confidence in security. Banking institutions losing money due to fraud are forced to raise interest rates and increase fees to their cardholders. The costs of fraud are passed to the banking institution's customers to offset the losses. The requisite to detect and eliminate fraud before it occurs is mutually beneficial to both the banking institution and cardholders. Credit card companies continue to focus on methods for identifying fraudulent transactions as they occur and on validating account owners. Financial institutions utilize various models to alert consumers of potential fraud on a real-time basis.

Current authorization models that validate the identity of the account holders during the transaction are limited or nonexistent. Many consumers are not required to provide any form of identification or signature proving identity for minimal purchase amount. For purchases requiring validation, consumers are able to validate a transaction with a simple, unverified signature mark at a merchant terminal. The introduction of the chip card added the additional element of security but can be combined with additional user authentication methods. To provide a more secure financial transaction, identity verification as a user authentication method can be realized through biometrics, most commonly, a fingerprint and can be achieved through the use of merchant touch screen credit card terminals or mobile purchasing applications.

Using a physical credit card embedded with a fingerprint positions the user authentication process at the point of sale, thus providing real-time validation of the user as the credit card account owner utilizing the biometric fingerprint as identity proof and signature. This research seeks to evaluate the biometric-enabled physical credit card in an effort to increase the level of credit card transaction security and reduce the occurrences of fraud.

PREFACE

Fraudulent credit card transactions can present themselves as stolen cards, copied cards, identity theft, theft of mobile devices, and online theft of credit card information. According to Fons et al, hacker and malware attacks accounted for 35 percent of the overall attacks (2006). Each source of fraud presents an opportunity for fraud and the possibility for a different detection model to be developed. The Federal Trade Commission describes methods that thieves use to commit fraud to include: low tech dumpster diving, high tech account hacking, dishonest clerks copying credit card information and disguised telemarketers seeking account information (Federal Trade Commission, 2015). “The inability to confidently verify the identity of a customer and their device leads to friendly fraud, which is defined as fraud perpetrated by a family member or close associate” (LexisNexis Risk Solutions, 2015, P. 1). In 2014, the highest number of data breaches worldwide, representing 72 percent overall, occurred in the U.S., (Nasdaq, 2014). “Counterfeit cards represented 37 percent of U.S. credit card fraud in 2014 with 14 percent in lost/stolen cards” (Nasdaq, 2015, P. 1).

The exploration of biometrics for verifying a user’s identity provides an opportunity for an additional layer of credit card security. Because the efforts to prevent fraud through EMV (Europay, Mastercard, Visa) chip cards and back-end fraud detection models are not providing actual user authentication, verifying the identity of a person at transaction initiation remains the most difficult but most important step in preventing fraud. While the EMV acronym was derived from a fraud prevention project in Europe during 1994 by Europay, MasterCard and Visa, the EMV trademark now includes the six, member organizations of EMVCo, including American Express, Discover, UnionPay, JCB, MasterCard, and Visa (Kobs, 2015). EMV chip represents a global standard for authenticating credit card transactions and is more commonly known as simply a chip card. Each credit card carries a computer chip inside the card, which aims to reduce counterfeiting by dynamically authenticating card transactions. The majority of fraud experts believe that the slow pace and lack of EMV adoption of chip cards by merchants in the U.S. has caused a disproportionately high amount of fraud (Nasdaq, 2015).

The importance of the analysis of detection models increases as additional variables are introduced from technological advancements in the devices used to make and receive credit card transactions, such as mobile devices and enhanced EMV chip credit card terminals. According to Nichols (2011), "Biometric identification enables the system to validate identity of an individual among many others without requiring any prior claim of identity (1-to-many). Typically, biometric identification consists of checking the inclusion of a user in a database" (pg. 24). Millions of credit card transactions are processed daily and require complex detection models in order to identify fraudulent transactions. Detection models must filter billions of lines of data to determine which transactions are legitimate. A variety of methods are used for identifying illegitimate transactions.

ACKNOWLEDGEMENTS

I would like to thank my dissertation committee, Drs. Elaine Seeman, Robert Chin, and Xiaolong Li, for their efforts in guiding and mentoring me in the completion of this dissertation. In addition to serving on my dissertation committee, they served on my program planning committee during my first half of the Ph.D. program and agreed, without hesitation, to continue on my dissertation committee. They provided me with significant insight into my research design. Dr. Elaine Seeman served as my dissertation chair and spent considerable time proofreading my work and encouraging me through the process. Each of these committee members was crucial to my success. Additionally, I would like to thank Dr. Mehran Shahhosseini for his guidance in preparing students for the proposal and defense of the dissertation.

My family deserves the utmost gratitude, and in particular, my husband, Jason, who filled my role at home so many times and never once complained. His encouragement and support kept me focused and fostered my success. I would like to thank my parents for raising me to have a determined spirit and perseverance. Without the support of my family, I would not have been able to complete the dissertation and achieve this great milestone.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Credit card fraud is a crime that exceeds physical and geographical boundaries and requires companies to remain steps ahead of criminals in order to prevent significant losses from impacting both the company and the card holders. Most credit card companies provide fraud protection in order to minimize losses to both card holders and credit card institutions. When a fraudulent transaction occurs, the credit card institution is often the initial entity on the receiving end of the financial loss; losses which are then passed on to the institution's customers. Numerous fraud detection and prevention methods exist to detect fraudulent transactions before they occur. Fraud detection models are generally considered company proprietary information, making the analysis of the various methods challenging.

Current credit card terminals require a physical card to be swiped and a PIN number or physical signature for validation purposes. The introduction of the (Europay, Mastercard, Visa) EMV chip card added the additional element of security by generating a unique code for the transaction that replaces the actual card number; however, the EMV chip can be combined with additional user authentication to prevent unauthorized users from initializing the transaction. The majority of credit card purchases are made with physical credit cards, and the lack of adequate identity proofing is a known security gap. Stolen cards can be swiped at a merchant terminal and used with nothing more than a forged signature, which is not always required. In this case, identity is verified simply by signature, which is not analyzed systematically to compare a valid versus an invalid signature. The question of “who am I?” is not sufficiently answered.

The chip card, combined with the user’s personal identification number (PIN), can potentially deter fraud and reduces the costs to companies of counterfeit cards. However, for stolen cards, the thief needs to know only the PIN number. According to the study by Matyas et al (2008), spying on customers while entering the PIN into the terminal can be done easily, particularly in crowded stores. Their study indicated that 35% of observers in a line could guess the PIN of the customer in front of them when using a PIN pad with security. In 83% of the instances, the participants could guess the PIN on the first try. When using a PIN pad without security, the observers could guess the customer’s PIN 80% of the time (Matyas, Krhovjak, & Kumpost, 2008).

Despite the efforts to prevent fraud through EMV chip cards and back-end fraud detection models, verifying the identity of a person at transaction initiation remains the most difficult but most important step in preventing fraud. The introduction of the iPhone 5 and the capability to lock and unlock the phone using a fingerprint was instrumental in cultural changes and the way biometric fingerprint authentication was viewed. Google Wallet and ApplePay capitalized on this feature, providing a way for financial transactions to be secured by using the fingerprint in the phone for authorization. “Since the release of ApplePay, banks and credit unions supporting ApplePay continue to rise to 400 financial institution partners in October 2015” (Papadimitriou, 2015, P. 1). ApplePay’s growth shows rapidly growing consumer demand in using biometrics when performing financial transactions. Financial institutions have the opportunity to capitalize on the culture shift and utilize a biometric-enabled physical credit card device to enhance the current physical card, leading to significant reductions in the amount of fraud related to counterfeit and lost/stolen cards.

Payments are a major driving force for the wide-scale global adoption of biometrics in the consumer market. Today, approximately 350 million people globally are using biometrics on a daily basis to provide secure, convenient user authentication and transaction authorization. The trend is expected to continue with a forecast of over three billion biometric payment users by 2020. Mobile payments, both in-apps and in-retail stores, have been a major contributor to the adoption of biometrics. The need for authentication speed coupled with the ability to include payment authentication to contactless payments has resulted in fingerprint biometrics becoming the standard (Goode Intelligence 2015).

The use of biometrics for credit card purchase authentication is achieved by imbedding the fingerprint into the credit card. The credit card is then activated upon touch. While various types of fraud detection models attempt to catch fraud as it occurs, successful identity proofing prevents the ability for a lost/stolen card to be used by an unauthorized user. Additionally, consumer demands can be met without requiring data storage of the biometric and without the legal implications of NPI data, subject to FCRA rules. The effectiveness of the biometric-enabled credit card must be greater than the overall concerns of consumers and must demonstrate the ability to prove the identity of the card holder at the time of purchase. The measurement of the reduction in fraud is subject to the ability to automatically disable a card if the biometric data does not match.

Statement of the Problem

Credit card fraud remains a problem for the financial industry and consumers, leaving financial institutions with the responsibility of developing techniques to identify potentially fraudulent transactions. Without proper verification of identity at the credit card terminal and no ability to control the merchant's role in checking customer identification through driver's licenses or other types of identification cards, financial institutions have relied primarily on software algorithms for preventing and detecting fraud. The problem for this study was to identify a solution to the lack of physical credit card authentication measures in order to combat credit card fraud and provide high authenticity identity proofing during credit card transactions.

Statement of the Purpose

The purpose of this study was to determine the reduction in the level of fraud, compared to the perceived reduction of fraud, by consumers for lost/stolen/physical cards when utilizing biometric-enabled credit card devices and without requiring a financial institution to store the biometric data in order to protect both consumers and financial institutions. The study will provide specific data related to the validity and feasibility of the biometric card, such as accuracy and error rates as well as fraud data comparisons, and consumer attitudes towards biometric credit cards. An evaluation of the data being passed in the background will determine the level of data privacy for the consumer.

Research Questions and Objectives

RQ1: Did the biometric-enabled device prevent a thief from using a counterfeit/lost/stolen card to make a purchase transaction?

RO1$_1$: Determine if lost/stolen cards can be effectively disabled by the inability to match the user with the card.

RO2$_1$: Determine if purchase transactions will fail at the credit card terminal when a lost/stolen card purchase it attempted.

RO3$_1$: Determine if fraud alerts can be triggered to the account holder after a failed attempt in using the biometric-enabled device to execute a transaction.

RQ2: Did the results provide evidence for the reduction in fraud using the biometric-enabled credit card device based on 2016 and 2017 physical card fraud rates?

RO1$_2$: Determine the level of overall reduction in fraud compared to 2016 and 2017 physical fraud rates when the use of a biometric-enabled device is applied prior to the user authentication process and at transaction initiation.

RO2$_2$: Evaluate the percentage of the marketplace expected to utilize the biometric-enabled device.

RO3$_2$: Evaluate the current levels of fraud related to physical credit card devices.

RQ3: Would the biometric-enabled device allow the consumer to maintain control over their biometric data?

RO1$_3$: Determine if the biometric-enabled device will store the biometric data (fingerprint) within the card and will not transmit the data through the merchant terminal, providing privacy and security.

RO2$_3$: Define the storage mechanism of the fingerprint data.

RQ4: Are consumers attitudes towards biometric credit cards supportive in order to reduce credit card fraud?

RO1$_4$ Evaluate the consumers' attitudes towards corporate responsibility in reducing fraud.

RO2$_4$: Evaluate the consumers' attitudes towards using a biometric credit card for purchases.

Statement of the Methodology

This study sought to provide an evaluation of a biometric-enabled credit card to be used by consumers for making credit card transactions at a contactless merchant terminal. A general evaluation of criteria, necessary for the implementation of the device and its usability with the average consumer, was performed, including biometric applications and data privacy concerns. The biometric-enabled device was proposed to increase the level of credit card transaction security and reduce the occurrences of fraud. The proposed method targeted the user authentication process at the point of sale to provide a real-time validation of the user as the credit card account owner using the biometric fingerprint as identity proof and signature. The study conducted was based on the current fraud levels for lost/stolen credit cards and did not include fraud related to online transactions in order to make a proper comparison of the expected reduction in fraud.

Enrollment Process

The first aspect of the study focused on the enrollment process to examine the effectiveness of the device in enrolling the card and the ability to execute purchase transactions. A biometric-enabled credit card was assigned and enrolled for numerous users of varying demographics. The enrollment process was limited to one person per card. Only one fingerprint could be associated with each card. Once successfully enrolled, purchase transactions were conducted for positive and negative scenarios. Positive scenarios were defined as transactions that are expected to be approved based on matching fingerprints. Negative scenarios were defined as transactions that are expected to be declined based on mismatching fingerprints.

Reduction in Fraud

Following the successful enrollment of a biometric-enabled device, an analysis of the expected reduction in fraud was conducted by gathering data from current fraud rates for lost/stolen cards and comparing to the data from the test transactions. Numerous test conditions were applied to test subjects with the enrolled cards in order to determine false positive and false negative rates in addition to expected positive and negative results. Based on the results from the test conditions, a comparison was generated against current fraud rates.

Data Privacy

The final portion of the study focused on data privacy pertaining to the biometric data required during the card enrollment process. Specific information was tested on the storage of the biometric data and transmission of data during transaction processing. Once the transaction was approved during the authorization process, transaction data logs were reviewed to determine the specific data elements being passed to the financial institution. The data privacy concerns are pertinent to address before considering the product for use in production.

Population and Sample

The population providing fingerprint data consisted of a convenience sample of 200 people from a shopping mall located in Glen Allen, Virginia. Participants in the study were selected without regard to demographic criteria. However, demographic criteria, such as age and gender, were analyzed as part of the user exit survey to determine future marketability. The use of a shopping location provides a strong sample of the population who would be using a physical credit or debit card and could be potential users of the biometric card. The same set of participants were asked to complete the survey instrument. The list of variables required for this study are shown on Table 1 and Table 2.

Table 1

List of Variables Required for Part 1: Biometric card registration and purchase

Variable Name	Variable Type	Data Collection Method
Successful Card Registration	Independent	Direct Report
Device False Negative	Dependent	Calculation of Number of Occurrences when Matching Fingerprints are Failed at the Merchant Terminal
Device False Positive	Dependent	Calculation of Number of Occurrences when Mismatching Fingerprints are Passed at the Merchant Terminal.
Number of Failed Fraudulent Transactions	Dependent	Calculation of Number of Fraudulent Transactions Failed Successfully Using the Biometric Credit Card
Number of Successful Transactions	Dependent	Calculation of Number of Legitimate Successful Transactions Using the Biometric Credit Card
2016 Fraud Rate	Control	Previously Published Data
2017 Fraud Rate	Control	Previously Published Data

Table 2

List of Variables Required for Part 2: Survey

Variable Name	Variable Type	Data Collection Method
Positive Fraud Experience	Dependent	Direct Report from Survey
Age Category	Dependent	Direct Report from Survey
Credit Card Ownership	Dependent	Direct Report from Survey
Biometric Card Device False Positive Result	Dependent	Direct Result from Experiment
Attitude Toward Identity Proofing	Independent	Direct Report from Survey
Fraud Perceptions	Independent	Direct Report from Survey
Ease of Use	Independent	Direct Report from Survey
Consumers’ Attitudes Toward Data Privacy	Independent	Direct Report from Survey

Instrument Creation and Validation

The survey instrument was created following Creswell's (2013) strategy for the development of a mixed methods study to incorporate the qualitative analysis with the quantitative analysis. This study focused on the consumer's attitudes towards fraud and the use of biometrics as a means to prevent credit card fraud in conjunction with the actual fraud detection rate when using the biometric card.

Statement of the Assumptions

The study made the following assumptions as parameters for success: 1) all participants have the ability to store a fingerprint; 2) the product does not violate compliance for the American for Disabilities Act (ADA); and 3) the study could be applied for future use in testing other biometric-enabled credit card devices for comparative analysis.

Statement of the Limitations

The study was limited to $1 - $5 purchases and, therefore, did not include conditions for which signatures would be required. Purchases under $25 are not authorized by the financial institution without customer signature unless the merchant or financial institution's agreement specifies otherwise. When the amount exceeds $25, the system triggers require a signature for identity verification. The conditions of the study were limited to purchases under the signature threshold and focused on the contactless readers' capabilities for a secure purchase. However, not making purchases over the $25 signature threshold limited the ability to test the biometric device's behavior when making larger purchase amounts. Changes in the authorization systems configurations would be required in order to deactivate the trigger for a signature and were, therefore, not included in this study.

Participant Bias

The completion of the survey by participants in the first phase of the study, biometric card registration and purchase, limits the scope of participants to only those with an interest in biometric credit cards. The assumption exists that participants expressing interest in the study would have an inherently higher level of acceptance of biometric usage for identity proofing. Therefore, the survey results could be skewed towards higher levels of acceptance for biometrics than if the survey was completed by non-participants in the biometric card registration, resulting in participant bias.

Specific Procedural Tasks

Detailed Test Conditions

Participants used the right thumb for enrolling the fingerprint on the card and must have no abrasions or dirt on the thumb throughout the study. During the testing of the biometric card at a merchant terminal, participants made a purchase between $1 and $5. The limit of $1 to $5 prevented the system from requiring a signature. Credit card companies have policies to require signature for purchases exceeding a specified dollar amount. The dollar amount threshold varies based on the credit card company.

Enrollment Steps – RQ1

(1) Enrolled 200 users with the biometric-enabled credit card using IDEX enrollment kit.

   a. Acquired 200 cards from biometric card manufacturer.

   b. Set up booth at Virginia’s Short Pump Town Center to attract participants.

   c. Registered each participant’s fingerprint to a single test card by waving the card over the contactless terminal, which provided power to the card, and successfully recorded the fingerprint data into the card.

i. The fingerprint selected for each participant was taken from the right thumb, unless the participant requested an alternate finger.

ii. The fingerprint was pressed onto the test card's fingerprint sensor chip and held there while waving the card over the contactless credit card terminal.

iii. The terminal automatically powered on when waved over the credit card terminal and captured the fingerprint image onto the card.

iv. The captured fingerprint resulted in the successful registration of the biometric credit for the card user.

d. The participant made a purchase at the booth using the contactless card reader, Ingenico iCT220; transaction results were recorded.

i. Purchases were made for the amount of $1 - $5. Participants placed their fingerprint on the biometric credit card and waved the card over the contactless terminal.

ii. Successful authentications would proceed to the confirmation of the amount on the merchant terminal screen.

iii. Once the amount was confirmed, the transaction moved to the authorization process. Successful purchases were approved.

e. The participants attempted to make a purchase on a card registered to someone else; transaction results were recorded.

i. Purchases were attempted for the amount of $1 - $5. Participants placed their fingerprint on the biometric credit card of a different participant and waved the card over the contactless terminal.

ii. Successful authentications would proceed to the confirmation of the amount on the merchant terminal screen. Unsuccessful authentications would result in a transaction error or decline message.

iii. If the authentication was successful, and the transaction amount was confirmed, the transaction moved to the authorization process. Successful purchases were approved.

(2) Created test conditions to satisfy the below requirements:

a. The card successfully read the fingerprint and matched the fingerprint to the test account holder.

b. The card successfully declined mismatched fingerprints.

c. The card was used at a merchant terminal successfully and authorized / declined transactions based on the fingerprint provided. Test cases varied in location, amount, merchant terminal type, and participant card used.

d. The card was disabled after three false attempts.

e. The card sent fraud alerts to the test account holder when card was disabled.

f. Ensured negative test conditions received expected results, irrespective of the control variables, false-positive and false-negative rates.

(3) The testing was executed by participants for each test condition. The results of the tests were documented and analyzed, including negative testing, to determine the level of accuracy and the ability of the biometric-enabled credit card to provide authenticity of identity.

Fraud Analysis Steps – RQ2

(1) Obtained previously published data for the years 2016 and 2017 for fraud rates as a percentage value of overall transactions.

(2) Determined the value for each of the measurement criteria used for comparison, e.g. usability, fraud detection accuracy, card disabled, fraud alerts.

(3) Performed an exit survey of each of the test users on their likelihood to use the product.

(4) Compared the test results for transaction failure and success rates against the expected results and calculated the fraud rate of the test cases. Compared the test study fraud rate to the 2016 and 2017 fraud rates.

Fingerprint Storage and Privacy Analysis – RQ3

(1) Enabled logging for the transaction authorization process.

(2) Monitored the logs for transaction data being sent to determine if any biometric data attempts to pass from the merchant terminal.

(3) Reviewed the construction of the biometric-enabled device and the storage of the fingerprint data, including the manner in which the device is powered to transmit the fingerprint data to the contactless terminal.

Consumer Perception Analysis – RQ4

(1) Participants completed the Biometric Credit Card Survey.

The survey was evaluated to determine consumer attitudes towards protecting their credit card accounts, corporations' role in protecting consumers from credit card fraud, and the perceptions of biometric credit cards in protecting credit card accounts.

The research study addresses the usability of the biometric card and the potential for fraud reduction. Biometrics as a means for identity proofing is not infallible, and establishing the types of errors and error rates using a biometric credit card will provide practitioners with data that can be used for determining the future direction of card configuration options. Consumer attitudes will have an impact on the success of the card in the marketplace despite the accuracy rates for biometric cards. The consumer attitudes from this study can be leveraged for future market analyses.

Definition of Terms

False negative biometric is defined as the negative result when a positive biometric match was provided.

False positive biometric is defined as the positive result when a negative biometric match was provided.

Identity proofing is defined by NIST as the resolve of a claimed identity to a single, unique identity through verification that the claimed identity is associated with the real person supplying the identity evidence.

CHAPTER 2

LITERATURE REVIEW

Sources of Credit Card Fraud

Before fraud detection models are created, understanding the sources of credit card fraud and their corresponding frequencies can help in determining the type of model that should be developed. The Federal Trade Commission describes methods that thieves use to commit fraud to include: low tech dumpster diving, high tech account hacking, dishonest clerks copying credit card information, disguised telemarketers seeking account information (Federal Trade Commission, 2015). ATM skimming, a procedure performed by copying debit card numbers as well as PINs using electronic devices (Williams, 2016) put customers at higher risk due to the usage of the PIN and cause losses into the billions across the financial sector annually. Regardless of the method used, once the thief has a customer's information, the role in detecting fraud becomes an additional responsibility of the credit card institution.

The United States accounts for the highest number of data breaches worldwide, 72 percent in 2014. Approximately 31.8 million U.S. consumers had their credit cards breached in 2014, which is more than three times the number affected in 2013. The majority of fraud experts believe that the slow pace and lack of EMV adoption, chip cards, by merchants in the

U.S. has caused a disproportionately high amount of fraud. EMV represents a global standard for authenticating credit card transactions. Each credit card carries a computer chip inside the card, which aims to reduce counterfeiting by dynamically authenticating card transactions. Counterfeit cards represented 37 percent of U.S. credit card fraud in 2014 (Nasdaq, 2015). Experian reported the exposed credit card numbers in 2017 totaled in excess of 14.2 million, an increase of 88% over 2016 (2018).

Mobile transactions are exceptionally at risk for fraud. Mobile transactions accounted for 14 percent of transaction volume in 2014 and 21 percent of overall fraudulent transactions, showing the high level of risk when utilizing mobile devices for purchasing transactions. Merchants who sell through mobile channels lost 70 percent more revenue due to fraud in 2014 than in 2013 (LexisNexis, 2015). Mobile transactions will continue to rise as smart phones introduce more purchase-friendly apps, such as Amazon and eBay's purchasing apps. However, physical cards are expected to continue to remain a dominant source of fraud. In 2017, credit card fraud persisted as the most common form of identity theft with over 133,000 reports. Children and teens are often targeted, and nearly 14,000 identity theft complaints were made to the Federal Trade Commission in 2017, representing approximately 3.9% of all identity theft complaints for the year (Tatham, 2018).

A Verizon risk team conducted a study in cooperation with the United States Security Service to analyze the sources of fraud impacting their company. The results of their study recorded approximately 900 million data breaches in financial institutions from 2008 to 2010. Hacker and malware attacks accounted for 35 percent of the overall attacks (Fons, Fons, & Cantó, 2006). Fraudulent credit card transactions can present themselves as stolen cards, copied cards, identity theft, theft of mobile devices, and online theft of credit card information. Each source presents an opportunity for fraud and the possibility for a different detection model to be developed. Regardless of the method used, once the thief has a customer's information, the role of detecting fraud is a responsibility of the financial institution.

Cost of Fraud

Globally, fraud is difficult to prevent based on the lack of merchant and credit card terminal device continuity. The EMV chip card implementation widely used across the United States to combat fraud has not been accepted worldwide (Knieff, 2016). According to LexisNexis (2016), chargebacks increased Year Over Year (YOY) by 3% in 2016. Additionally, the physical point of sale channel costs per dollar of fraud losses was $2.38 in 2015 and rose to $2.46 in 2016 as shown in Figure 1. These increases display a level of fraud risk that continues to increase after the implementation of EMV adoption combined with behavior-based algorithms for fraud detection.

In the year 2016, approximately 15 million consumers were victims of identity theft or credit card fraud, but card-not-present fraud represented the largest increase of 40% compared to the year 2015 (Grant, 2017). The level of fraud as a percentage of revenues between 2015 to 2016 increased from 1.32% to 1.47% despite EMV adoption (LexisNexis, 2016). While card-not-present transactions are less secure than card-present transactions, the card-present fraud levels related to lost/stolen cards are increasing 6% per year (Steele, 2017). Card-present fraud extends to identity theft and card-not-present fraud. Once the thief obtains the card, the transaction can easily move from a purchase in a physical store to an online purchase.

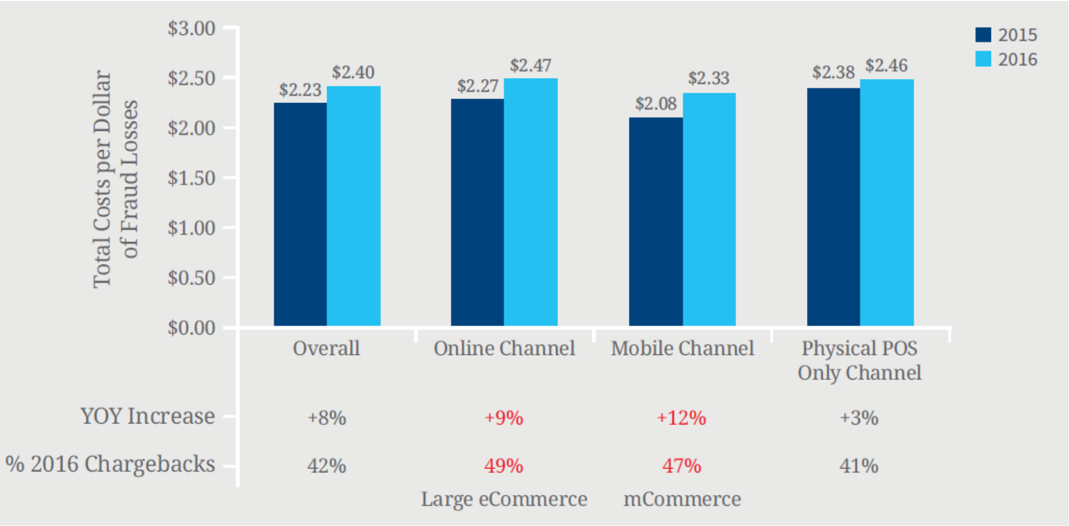


Figure 1

2016 LexisNexis True Cost of Fraud Study

In a global consumer card fraud study performed, 39 percent of respondents (of 4,813 participants) had experienced fraud in the past five years. In 2016, this number had jumped to 46 percent despite growing efforts to develop prevention mechanisms, such as enhanced behavioral algorithms and EMV chip cards (Knieff, 2016).

Fraud and Litigation

Numerous litigations have been filed for misuse of personal information and the lack of protections for PII data. As hackers continue to breach systems housing personal data, information security policies become more crucial in order to protect individuals and consumers. Cyber security departments are increasing in size in order to stay a step ahead of the criminal hackers, who seek to infiltrate companies' systems to gain customer data. In January 2002, the case of United States v. Llera Plaza, the judge ruled on the admissibility of fingerprints as a form of identification meeting the requirements of scientific evidence. This ruling, while directly applied to criminal investigations, gives credence to the uniqueness of fingerprints in their applications in forensics. Digital forensics and the use of the fingerprint impacts the individual's privacy beyond the consumer standpoint (Kaye, 2003).

Amar Singh was one of four leaders in the Operation Swiper identity theft attack that included 111 individuals based in Queens, NY and operating across Europe, Asia, Africa, and the Middle East. Singh was charged with stealing personal credit card information from thousands of European and American citizens. Singh was accused of stealing approximately $13 million dollars and was further accused of identity theft and enterprise corruption. Part of the operations included facilities for making counterfeit driver's licenses using the stolen identities. Skimmers and other card reader devices were used to fraudulently obtain the credit card information of consumers (IDCPI, 2013).

The case of Amar Singh is representative of the grave nature of crimes related to credit card fraud and identity theft. While laws have been created to penalize criminals committing these offenses, the privacy of individual's data continues to be at risk. As new technologies seek to utilize other forms of identity verification and proof, such as biometrics, the data could be subject to theft by hackers who are able to create devices to copy data. Identity theft will likely not go away but become more complex as biometrics are introduced as a more widespread form of identity verification. The thieves and hackers will develop more complex mechanisms for copying and retrieving the data, which could result in long-term issues for individuals (Spraggs, 2007).

Credit Card Authorization Process

A typical authorization begins at the point of sale when the credit card is swiped at the terminal. Once the customer swipes the EMV chip card and enters the correct PIN, the authorization goes online to the banking institution. A string of data, found on Table 3, is sent to the banking institution providing information about the authorization. Additional information is gathered about the customer by matching the customer's account and retrieving additional data regarding the customer's recent address changes, card requests, available credit, fraud score, etc. The authorization responses to the merchant for each transaction are as follows: Approved; Declined or Card Not Accepted; Call, Call Center, or Referrals; or Pick Up. Merchants are advised by the card issuer of different actions based on each authorization response. If the customer's account is in good standing and enough credit is available to support the transaction, the authorization will proceed to a system for fraud detection (Visa, 2015).

Table 3

Authorization Data

Description of Data	**Example Data Set**
Entry Method Code	Chip
Merchant Name	Sweet and Spice Bakery
Merchant City Name	Los Angeles
Merchant State	California
Merchant Country	USA
Authorization Amount	$22.49
Customer Account Number	4744-7800-1111-1111
Customer Home Postal Code	98649

Network Communication Protocols

As data passes through the network, data is encrypted between the client and server to ensure the credit card numbers and PII is not at risk for interception. Two protocols commonly used for processing credit card payments are ZVT and Poseidon. ZVT is used between point of sale (POS) systems and the card readers. However, Poseidon, is used between the card reader and the merchant's bank. Both of these protocols introduce a potential for network intrusion (Bright, 2015).

Originally, the ZVT protocol was created for serial port connections but is frequently used over wired and wireless Ethernet. Authentication is not required between the POS and the card reader; therefore, a positive or negative proof of identity can be generated by an attacker posing as a man-in-the-middle (Bright, 2015). Traditional cards using the magstripe represent the highest level of risk with this type of attack. The attacker could not only read the magnetic stripe data from the card but could request the PIN, gaining immediate access to the credit card.

Cloned cards could be created for future use by criminals. Counterfeit cards created from these types of attacks contributed to the creation of the EMV chip card. Poseidon, global standard ISO 8583, does not require strong authentication. A purchased card reader could be configured to pose as the victim and successfully process transactions. Both ZVT and Poseidon create fraud risk due to lack of highly secure authentication mechanisms (Bright, 2015).

Two-Factor Authentication

The smart card uses the two-factor user authentication mechanisms based on the physical smart card and password, known as the password authentication scheme. In this scenario, a secure server/client relationship issues the personalized smart-card and initial password. The password that is registered to the card allows the client to access the server during the authentication process. The security goal is to ensure mutual authentication between client and server. When conducting a transaction, the client is required to have in possession the smart card and successfully provide the password for successful authentication (Visa, 2015). This process is known as two-factor authentication. EMV/chip cards provide an additional layer of security using the embedded micro-computer chip. Payment data is more secure on a chip-enabled payment card than on a magnetic stripe card, as the chip supports dynamic authentication, while the magnetic stripe does not. Consequently, data from a traditional magstripe card is static and can be easily copied, a process referred to as skimming (Clark, 2011).

Elements of the Biometric Credit Card

This entire process is without the element of a biometric authentication. When adding a biometric, two types of biometrics can be selected for authentication. The first type is a biometric credit card that sends the biometric data along with the other transaction details and is validated as another piece of data against the banking institution's customer data. The biometric data, a fingerprint, is labeled as Personally Identifiable Information (PII) and is subject to high levels of sensitivity and protection. Because of the sensitivity/confidentiality of the data, the second type of biometric credit card was created that allows the fingerprint to be stored and validated on the card without sending the fingerprint to the banking institution, making it the preferred option; see Figure 2 (Zwipe, 2016).

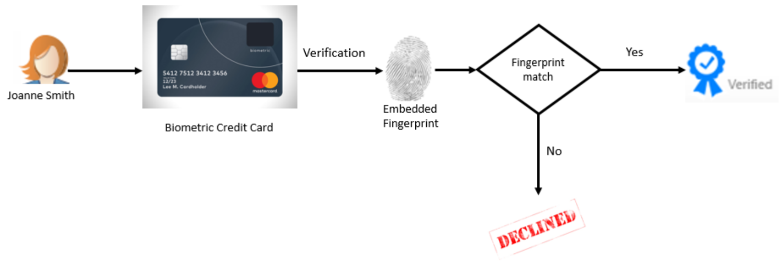


Figure 2

Representing the interface between the user and the biometric credit card

The biometric credit card includes the current technology of the chip and comprises and embedded image of the account holder's fingerprint. The embedded fingerprint image is compared to the actual fingerprint when the finger is placed on the credit card and activated through a contactless terminal. The verification of the biometric credit card would only be enabled when the card is swiped across a contactless credit card terminal. The lack of required built-in batteries in the biometric card necessitates a contactless terminal for power. Once the card is swiped over the terminal, the user must place their pre-registered finger on the card for verification. If the fingerprint is a match, the credit card payment will begin authorization. If the fingerprint is not a match, the card will not begin payment authorization. The card cannot be used until a fingerprint match is successful. The successful match completes the authentication process and enables the authorization process to begin; however, the fingerprint data will not be sent as part of the authorization data (Green et al., 2018).

The biometric cards operated via Micro-Electronic-Mechanical Systems (MEMS) chips embedded in the card, using capacitive fingerprint sensors, capturing the pressure sensitive contacts as pixels on the sensor's surface. Each pixel is a capacitive pressure sensor that has a MEMS cavity structure stacked on a Complementary Metal–Oxide–Semiconductor Large-Scale

Integration (CMOS LSI). Beneath each cavity structure are sensing circuits. The sensing circuits electronically detect the fingerprint ridges when the finger is pressed onto the underlying film of the cavity structure. Power is provided directly to the card using when holding the card above the merchant terminal (Tang, 2018).

Most fraud systems rely on behavior analysis algorithms to detect unusual activity on the credit card based on complex rules. If the result of the algorithm indicates potential for fraud, then the transaction is declined. While the system is performing all of the validations in the background, the customer is waiting at the merchant terminal for the transaction to be approved. The few seconds that pass between the time the customer enters their PIN and the approve or decline message may seem lengthy, but many validations are occurring at the banking institution (Raj & Porta, 2011).

Identity Proofing & Spoofing

The National Institute of Standards and Technology (NIST) 800-63A identifies three layers of identity assurance levels (IAL) in order to verify the claimed identity of the individual. IAL1 determines the attributes provided throughout the individual's activities are self-asserted, without validation or verification. The physical, in-person or remote identification of a person provides evidence of the person's true existence in the real world, as referenced in IAL2. However, the required physical presence of the person is required in IAL3 for verification of the person's attributes. Following the standards set forth by NIST provide assurance of the subject's claimed identity.

The expected results of an identity proofing incident as defined by NIST 800-63A are as follows:

> “Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves; validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated); validate that the claimed identity exists in the real world; verify that the claimed identity is associated with the real person supplying the identity evidence” (Grassi & Fenton, 2017).

As shown in Figure 3, the goal of identity proofing is to provide assurance that the claimed identity of a person is the person’s actual identity. While NIST 800-63A provides guidelines specifically for credential service providers to verify identity, the standard notes the difficulty in providing verification of digital identity where physical presence is not available. Financial or online transactions limit the ability to provide the same level of in-person identity proofing, causing challenges for ensuring the transactions are not fraudulent.

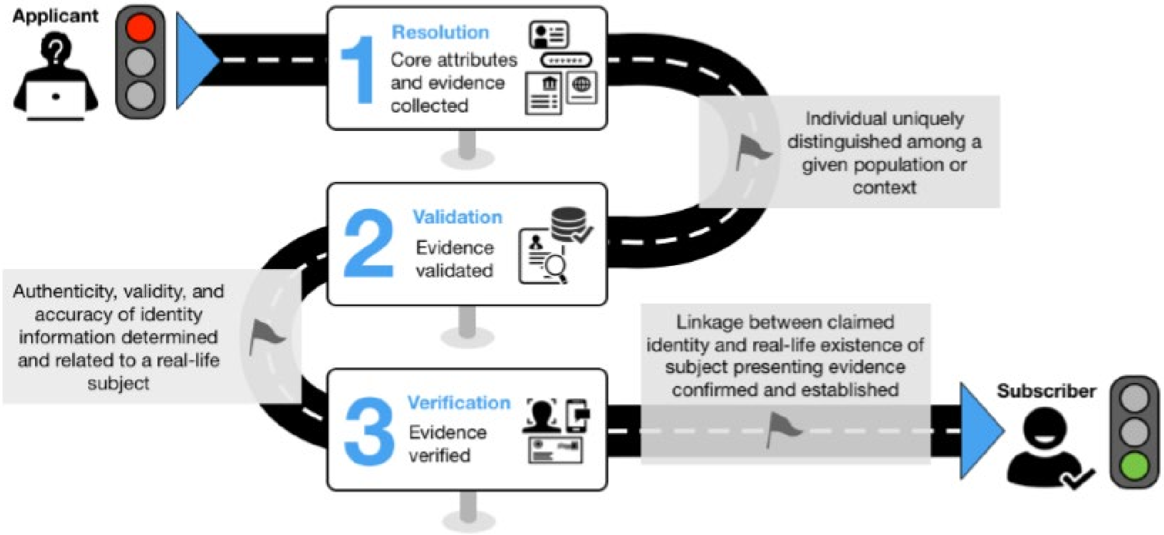

Applicant
1
Resolution
Core attributes and evidence collected
Individual uniquely distinguished among a given population or context
2
Validation
Evidence validated
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject
3
Verification
Evidence verified
Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established
Subscriber

Figure 3

The identity proofing and enrollment flow (NIST, 2017)

Identity proofing is typically resolved by using a three-way verification of 1) something you know, 2) something you are, and 3) something you have. Utilizing a biometric credit card provides something you are with something you know. If a PIN number is required in conjunction with the biometric card, the identity proofing is then strengthened by its use of all three verifications.

Fingerprints have been used as a means of identity proofing with law enforcement for decades, but the old adage of, *fingerprints cannot lie, but liars can make fingerprints,* is indicative of new security threats imposed when using biometrics for identity proofing. Using biometrics allows a person's individual attributes to serve as the key, but those attributes are still subject to theft. Tutorials can be found on web sites with instructions for lifting fingerprints and creating masks for deceiving biometric validation systems, such as can be found on the Law Enforcement Magazine Website (Spraggs, 2007), providing guidance on the tools and method used for pulling fingerprints from a plain surface. Ensuring these simple methods cannot be used to create a fraudulent biometric credit card requires anti-spoofing procedures as part of the biometric card design.

Fraud Detection Models

Banking institutions losing money due to fraud are forced to raise interest rates and increase fees to their cardholders. These costs from fraud are passed on to the banking institution's customers to offset the losses. The need to detect and eliminate fraud before it occurs is mutually beneficial to both the banking institution and cardholders. Detection models vary from organization to organization and incorporate a variety of methods, creating dynamic models that track and evaluate customer behaviors to data mining techniques and alert messaging. The exploration of biometrics for verifying a user's identity provides an opportunity for an additional layer of credit card security.

The importance of the analysis of detection models increases as additional variables are introduced from technological advancements in the devices used to make and receive credit card transactions, i.e. mobile devices, enhanced chip credit card terminals. Millions of credit card transactions are processed on a daily basis, requiring complex detection models to be able to identify fraudulent transactions. Detection models must filter through billions of lines of data to determine which transactions are legitimate. A variety of methods are used for identifying illegitimate transactions. Most fraud detection models analyze the transactional data during the transaction processing or afterward.

Dempster-Shafer Behavior –Based Model

A large number of detection models are behavior-based, using algorithms to analyze spending behaviors. The Dempster-Shafer theory described by Raj and Portia uses a fusion approach, combining evidences of past and current shopping behavior (Raj & Portia, 2011). When a purchase in progress falls out of acceptable deviation of spending patterns, the transaction can be denied, and the customer can be alerted of the potential fraud. Alerts can be in the form of a phone call from the company, an email, or a text message. In such cases, the customer has the opportunity to provide personal information to validate their identity with a customer service agent and proceed with the purchase.

In the Dempster-Shafter theory, the BLAH-FDS is a hybrid of BLAST and SSAHA algorithms, using a two-stage sequence alignment to analyze past spending behaviors (Raj & Portia, 2011). The profile analyzer establishes a profile of the consumer based on past and present spending patterns. An additional deviation analyzer looks for past fraudulent behaviors, and a comparison of the two analyzers is performed. If the comparison yields a potential fraud, alerts can be triggered (Figure 4).

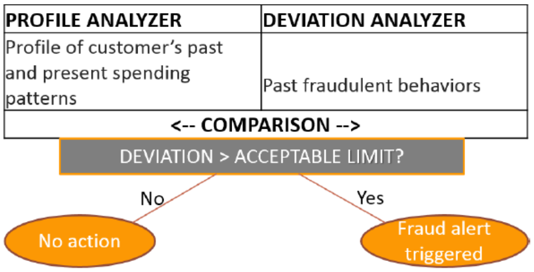

PROFILE ANALYZER
DEVIATION ANALYZER
Profile of customer's past and present spending patterns
Past fraudulent behaviors
<-- COMPARISON -->
DEVIATION > ACCEPTABLE LIMIT?
No
Yes
No action
Fraud alert triggered

Figure 4

Dempster-Shafter Theory

Patterson's Universal ID and Biometrics

Patterson proposes a method using a universal identification number (UID) and biometric data for validating receipts on a payment processing network (Patterson, 2010). Patterson's model uses three identifiers that must match in order to authenticate a user. The first identifier can be an account ID or bank identification number, coupled with the second identifier as biometric data. The two identifiers are then sent to an identification system to detect predetermined correlation, such that the data received matches stored data. This process of predetermined correlation describes the identification system that receives the authentication request message and compares the UID and biometric data to a second set of data to determine if a match exists (Patterson, 2010).

In Patterson's model, the user inputs a card into a Micro-ATM terminal and uses biometric data to authenticate that the data matches the system ID for payment processing. While Patterson's model thoroughly depicts a relationship between a UID and biometric data, the model can be further extended beyond payment processing and micro-ATMs to credit card purchasing transactions. Patterson's usage of a UID for associating biometric data requires a separate identification system, external to the customer data in the source of record, for matching the biometric data provided by the user to the data associated with a customer. The use of biometrics at the entry point of the transaction allows for detection of fraud before the transaction is executed.

Moganeshwaran's et al. Fingerprint-Fingervein Multimodal Biometric Authentication

Moganeshwaran proposes a multimodal authentication using more than one biometric input for verifying user identity (Moganeshwaran, Mohamed, & Suhaini, 2012). Their model suggests an increase in probability of user authenticity when two or more biometric data are provided. The data could be more than one fingerprint, veins within the finger plus a fingerprint, hand vein, or multiple snapshots of the same biometric data (e.g. three templates of right index fingerprint). Moganeshwaran states several advantages of the multiple biometric authentication system, such as the following: it can overcome the non-universality, is less affected by noise, provides a stronger security environment, and improves matching accuracy (Moganeshwaran, Mohamed, & Suhaini, 2012).

The fingerprint authentication system has high authentication rate, but the captured images are susceptible to noise (Moganeshwaran, Mohamed, & Suhaini, 2012). Additionally, the fingerprints can be smudged, damaged, or forged, as noted in Figure 5. The quality of fingerprints, Figure 6, can vary and create the potential for a denial or rejected authentication, resulting in a false negative. False negative results of a biometric match, when being used for a credit card transaction authorization, can cause erroneous transaction denials.

Figure 5

Captured fingerprint smudges

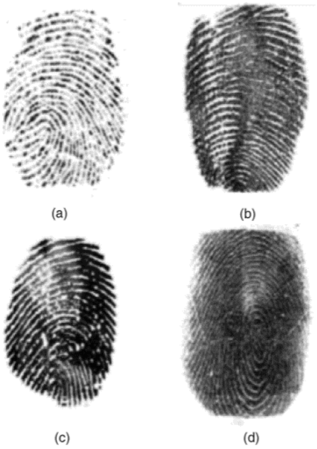


Figure 6

Fingerprint quality comparison

Moganeshwaran suggests fingerveins for higher authenticity, as the vein is located underneath the finger and is difficult to forge or steal. The error rate must be considered as a factor for measuring the need for multimodal, further validated by the measured rate of .33 percent error in contrast to 2.21 percent error with fingerprints alone (Moganeshwaran, Mohamed, & Suhaini, 2012). Using the multimodal biometric model requires more than one biometric input by the customer. Capturing multiple modes of biometric data when making a credit card purchase is not a cost-effective method. Merchants may be unwilling to participate in capturing the information. Customers may be resistant to provide personal information for a simple purchase.

Storing biometric data is averted using the biometric credit card. Not only would the storage be a security and privacy concern, but biometric databases are considered a big data problem with biometric templates ranging from 256b to 3KB and raw images of 16KB to 300KB. One of the challenges to overcome with biometric data is the noise level and the computational costs incurred when processing the data. The majority of traditional biometric systems operate with restrictions on the size of their biometric data due to the storage limitations (Pal & Wang, 1996).

Embedded Biometric Sensors

The biometric card must first be registered to the user, which is part of the card's built-in access control system. This initial process is performed by fingerprint sensor enrollment, whereby the merchant terminal acts as the enrolling station for sensing the fingerprint and supplies the power to the card directly. The ridges and valleys of the fingerprint are recorded on the device as the authorized person based upon the sensed fingerprint, and the captured image is framed, digitized, and stored as a static digital image. The biometric card is essentially the access triggering device, carried by the authorized person, and an access controller for granting access to an authorized person bearing the access triggering device (USA Patent No. US5903225 A, 1997).

The biometric card uses a contactless terminal and operates using a wireless transmitter, which is built into the biometric card. The wireless transmitter, a passive transponder, transmits the authorization signal of pass or fail based on the registered card's stored authorization data. Embedded in the biometric credit card are fingerprint sensors or transducers of simple structure. The transducers are capable of detecting and sensing the patterns contained in the skin structure of the human finger. When the fingerprint is pressed against the card and swiped over the terminal, an electric output signal is delivered in accordance with the pattern of ridges and valleys of the finger.

Typically, the access controller includes a wireless receiver, such as including a transponder powering circuit, for receiving the authorization signal and granting access responsive to the wireless transmitter being in proximity to the wireless receiver (Schmitt, 1997). Biometric data is not being sent to the banking institution as part of the authorization data. The authorization will occur immediately as part of the card's built-in access verification controls. A major advantage is the elimination of the fingerprint as personally identifiable information (PII) owned and maintained by the financial institution.

Similar functionality is notable in ApplePay's use of fingerprint sensors for providing identity proofing as part of the transaction authorization. A key contrast is the use of the optical fingerprint scanner for both registration and enrollment as well as user verification. Similar to the biometric card, matching credentials are stored on the phone, acting as a portable memory device to the user's physical characteristic, the live fingerprint. Contrary to the perception of most users, the fingerprint stored in ApplePay is not sent to the financial institutions.

An additional component of anti-fraud techniques gained through ApplePay is the identification of heat consistent with a human's body temperature. The biometric read determines whether the object exhibits characteristics of blood flow comparable to a live human. According to Shinder (2001), an imposter finger can fool the disclosed devices using this approach by deceptively simulating blood flow. The use of flashlights or motion can defraud the system, because devices detect variation in levels of reflected light energy from the object being scanned as evidence of blood flow.

Biometric Validation Accuracy

An analysis of biometrics verification was performed by Ruiz-Mezcue (1999) in a real environment for teleservices cash dispensers to measure the effectiveness of voice and facial recognition in user identification for ATM transactions using different hardware architecture. The verification included imposter's claims and positive matches. The facial and voice recognition method provides a variation of using multimodal biometric user authentication, but the practicality of multimodal biometrics is far less valuable for merchant credit card transaction terminals.

The ability to validate the fingerprint with high level of accuracy is crucial to the success of biometric authorization. If the fingerprint is not aligned correctly, a different finger is used, or the image is rotated, this will lead to a declined credit card transaction. Back-up processes would need to be in place to ensure identity verification can be established via alternative means.

"Minutia-based (fingerprint ridge discontinuities: ridge endings and ridge bifurcations) is the most widely used technique due to its good performance with less computational costs (processing time and memory needs) than other techniques; matching two fingerprints in minutia-based representations becomes a point pattern-matching problem, and it consists of finding the alignment and correspondences between pairs of minutiae points in both sets", (Fons, Fons, & Canto, 2006). Distortions in fingerprints can be caused by a cut, bruise, or laceration to the finger as well as dirt. Areas with significant distortion where a large area of the fingerprint has been compromised can lead to the creation of spurious minutiae, resulting in a large area to be ignored and a large error in localization (Hong, Wang, & Jain, 1998). Compared to a single biometric system, the extraction of multiple biometric features reduces the error rate and leads to improved performance of an authentication system (Esan & Ngwira, 2013).

Biometric Card Feasibility Analysis

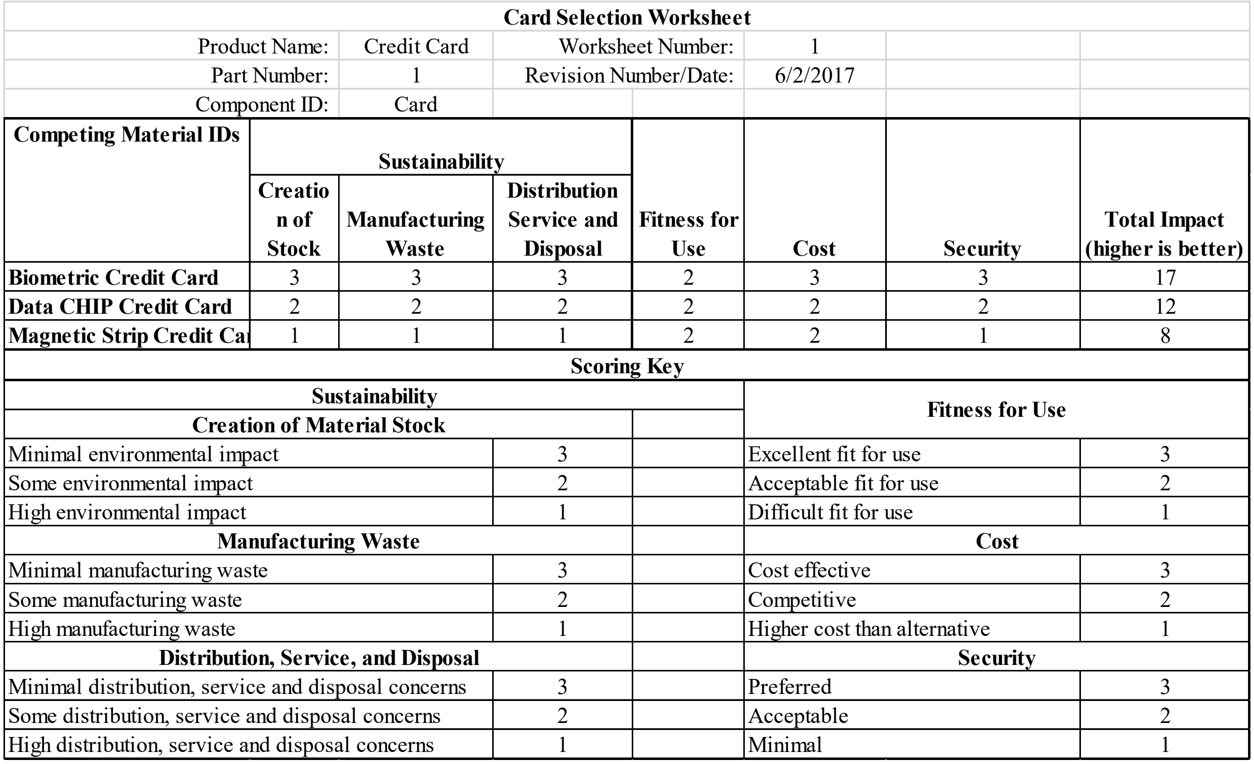
A general evaluation of criteria necessary for the implementation of the device and its usability with the average consumer is performed for the regular mag strip, the chip card, and the biometric card. The biometric-enabled device is proposed to increase the level of credit card transaction security and reduce the occurrences of fraud. The biometric card targets the user authentication process at the point of sale to provide a real-time validation of the user as the credit card account owner using the biometric fingerprint as identity proof and signature.

Profitable and Compliant Valuation Chart

In evaluating the various credit cards available for purchase and the value each provides to customers, a value chart, Table 4, provides measurable criteria for determining the type of card that offers the highest value to improve customer experience, profitability, and long-term sustainability.

Table 4

Profitable and Compliant Valuation Chart



Card Selection Worksheet					
Product Name:	Credit Card	Worksheet Number:	1		
Part Number:	1	Revision Number/Date:	6/2/2017		
Component ID:	Card				

Competing Material IDs	Sustainability						
	Creation of Stock	Manufacturing Waste	Distribution Service and Disposal	Fitness for Use	Cost	Security	Total Impact (higher is better)
Biometric Credit Card	3	3	3	2	3	3	17
Data CHIP Credit Card	2	2	2	2	2	2	12
Magnetic Strip Credit Ca	1	1	1	2	2	1	8

Scoring Key				
Sustainability			Fitness for Use	
Creation of Material Stock				
Minimal environmental impact	3		Excellent fit for use	3
Some environmental impact	2		Acceptable fit for use	2
High environmental impact	1		Difficult fit for use	1
Manufacturing Waste			Cost	
Minimal manufacturing waste	3		Cost effective	3
Some manufacturing waste	2		Competitive	2
High manufacturing waste	1		Higher cost than alternative	1
Distribution, Service, and Disposal			Security	
Minimal distribution, service and disposal concerns	3		Preferred	3
Some distribution, service and disposal concerns	2		Acceptable	2
High distribution, service and disposal concerns	1		Minimal	1

Sustainability

The environmental and sustainability impact of the card selection process revolves around three main categories: creation of the stock material, waste removal involved with the manufacturing process, and resources necessary to distribute, service, and ultimately dispose of the card stock.

Creating of the Material Stock

The raw materials involved with creating the card itself is a variation of Polyvinyl Chloride Acetate (PVCA). The primary base chemicals in this process are byproducts from the petrochemical industry when making different grades of gasoline. Other industries which supply this raw material are the Natural Gas and even Biomass industries. By combining vinyl acetate and vinyl chlorides, sheets of PVCA are formed as a base stock. These sheets of PVCA are then sent to the card manufacturers which use a variety of thermoforming processes in order to create individual cards out of the base stock. Additional components to the cards include adding dye to the base stock, applying text and graphics to the cards, as well as adding laminating magnetic strips, microchips, and even pressure-sensitive striping material to the cards before an outer laminate layer is applied (Randall 2015).

The PVCA is 100% recyclable, but the magnetic strips, microchips, and pressure-sensitive tape will have to be separated from the card stock during the recycling process. Unfortunately, most recyclers do not currently accept these small cards as recyclable materials, and it is estimated that 75 million pounds of credit and gift card waste ends up in landfills each year (Mazzoni 2013). Because the majority of the base material is a byproduct of the oil industry and the majority of the credit cards themselves are recyclable, the measure for sustainability of material stock will be to issue fewer credit cards to customers. Combining all the data on one card and making the cards more secure so that fewer cards are issued each year will have the biggest impact to material stock sustainability.

Manufacturing Waste

Manufacturing waste is minimal in all versions of the credit card manufacturing processes. However, the cost of getting each card to the customer can be substantial when the hundreds of millions of cards that get issued each year are considered. The cost to manufacture just one card will range from $1.00 to $2.00 per card. According to Frellick (2010), by adding a microchip to each card, the added cost of the card manufacturing process ranges from $0.10 to $1.00 per card. Because of the additional process involved with creating unique credit cards and tracking those cards all the way to the customer, the total cost of a card can range from $1.11 to

$2.00 per card (Frellick 2010). To compare, enhanced version of the standard credit card known as Europay, Mastercard, and Visa or "EMV" utilize "chip and pin" security and cost between $2.00-$2.25 to produce. The overall cost for manufacturing, processing, and delivering the biometric credit card is estimated at nearly three-times more than the standard card, at an average cost of $3.00 per card.

Distribution, Service, and Disposal

All three credit card types incur similar servicing costs for the initial card when it is issued. However, the cost to repeat that process is what separates a good, sustainable choice from one that has recurring costs. A customer who has to call to cancel or change a credit card will add wasted effort to the credit card system by tying up a human to process the order, the manufacturing systems to create another unique card, and the distribution channel to supply a new card to the customer. The most sustainable systems for credit cards are ones in which less cards are issued each year.

Biometric Credit Cards Implementation & Manufacturing Costs

Significant costs must be considered when implementing and utilizing biometric credit cards for commerce. From a manufacturing perspective, before a credit card can be disseminated to the end-user, it must travel through a comprehensive set of processes facilitated by multifarious machinery with complex security measures (Frellick 2016).

Costs to Retailers and Customers

The first set of costs is associated with merchants that provide goods and services. The good news is that businesses presently utilizing proximity card readers, or smart card readers, now have the opportunity to add biometric authorization to their transaction verification process without having to purchase expensive biometric readers. However, merchants currently using traditional mag stripe card readers will need to upgrade to contactless terminals at several hundred dollars per unit with the possibility of a full upgrade of their entire point of sales system. Aside from the upgrade to contactless credit card terminal equipment, merchants will have little additional costs. The contactless terminals do not require additional training for personnel before biometric transactions can be accepted, equating to minimal training costs for business electing to accept the form of payment. Small businesses and organizations with limited resources may be hesitant to make the initial investment in the contactless terminals and could face the prospect of lost sales.

Additional lost sales could occur due to malfunctioning equipment. Malfunctions can occur when attempting to scan the biometric credit card to process the transaction, leading to significant delays in processing the payment transaction or failures due to false rejections. If the biometric card and corresponding technology fail at the credit card terminal and cannot accurately identify the user, the payment method is useless (Schaffer 2015). Jain and Angus (2013) state that 80% of consumer spending in the United States is cashless (Schaffer 2015). With such a major reliance on cashless transaction methods, seamless integration of the biometric credit card technology with existing credit card technologies will be paramount.

Paying for Security and Peace of Mind

Mastercard and Zwipe partnered to pilot Zwipe's biometric credit, which resulted in positive feedback from customers and retailers. According to Zwipe's founder and CEO, Kim Humborstad, "Cardholders love how easy the card is to use with the added security feature. We have also had exceptionally good reaction from retailers participating in the pilot" (Chowdhry 2014). When considering the enhanced security features of the biometric credit card, bank clients are willing to pay additional user fees for enhanced security to combat identity theft. For example, as early as 2006, a Unisys survey indicated that approximately 40 percent of citizens are willing to pay fees for more protection, and biometrics is the preferred method for combating fraud (Inside Arm 2006).

Implementation

In order to implement the biometric-enabled credit card, merchants must provide a contactless credit card terminal in order to read the card. Credit card institutions will be required to adopt enrollment processes that ensure account holders can successfully enroll the fingerprint on the sensor located in the card. Additionally, consumers who desire the card may be required to pay a minimal fee for the purchase of the card to compensate for the additional initial cost of manufacturing. Due to ease of the product, the implementation of the card will not require substantial additional steps above the rollout of credit card products, such as the chip card. The implementation will yield immediate results for fraud protection.

Given the overall benefits of cost reduction for the merchants, credit card institutions, and average consumers, the added security of financial data through the use of the biometric-enabled credit card reduces the fraud and identity theft risk for both consumers and credit card institutions. Additionally, the consumer can maintain the protection of their privacy using an integrated biometric fingerprint sensor that is built into the smartcard. The combination of the existing chip card with the biometric credit card provides enhanced security and convenience for consumers.

Corporate Responsibility to Consumers

Privacy protections of the data are the responsibility of the party collecting the information from the individual/consumer and are a serious concern in the design of biometric identity proofing and authentication systems. The uniqueness of the traits increases the criticality of protecting the data. When considering privacy, the value of security and convenience typically supersedes the value in safeguarding biometric data. During the authentication process, a user claims an identity by providing biometric information to a system for comparison against the stored references. In the case of surveillance applications, the process differs only that the system initiates the comparison rather than the user (Krishnan & Sy, 2012).

Companies, such as Busch Gardens and Disney Theme Parks, collect biometric data for entrance to the park in effort to track members and limit the membership fraud resulting from sharing of annual membership cards. The membership systems store the member's fingerprint data as well as photographs. Upon park entry, a member must scan the same finger each time, which is compared to the fingerprint in the system for a match. If authenticated successfully, the member gains entry into the park. Additionally, photographs of the members are stored to ensure the photograph on the account record matches the person entering the park. In these cases, the theme parks have the responsibility for storing and protecting the biometric data of their members. Their cybersecurity measures become critical components in the protection of this data.

Numerous governmental programs utilize biometric data, specifically fingerprint data, such as First Capture. First Capture is a multi-agency governmental program working to develop technology designed to capture ten rolled-equivalent fingerprints in less than 15 seconds. The focus is to ensure high quality of the fingerprint image with a device that is portable. The Integrated Automatic Fingerprint Identification System (IAFIS) contains over 47 million fingerprints and includes the electronic exchanges of fingerprints (Melodia, Bond, &

Angelovska-Wilson, 2015). Governments have equal responsibility in maintaining and protecting biometric data.

The IAFIS is used by the FBI Criminal Justice System in order to accelerate the process of performing a fingerprint search. When performed manually, the search took up to 90 days, but when performed electronically, the search could be completed within two hours for criminal requests. The National Institute for Standards and Technology (NIST), Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, outlines the criteria for formatting and storing electronic fingerprint images as well as the specifications for the devices used to collect the biometric fingerprint images (Melodia, Bond, & Angelovska-Wilson, 2015). Storing procedures is critical in ensuring that proper cyber security methods are used in data protection. A lapse in following the procedures could result in data penetration and leakage of personal information.

Apple's iPhone 6 offers the capability for users to password protect their phones using a fingerprint. The fingerprint is stored locally and is not shared with Apple, Inc. The fingerprint can be used to authenticate purchases at a contactless credit card merchant terminal, but the fingerprint is not passed in the system during the authentication process. The protection of the fingerprint data is a feature provided by Apple that is unique. The fingerprint's extensive level of protection from unauthorized access was an area of focus for the U.S. government when they attempted to hack into Apple's code to try and find a pathway to unlock a user's fingerprint-locked phone. The case between the FBI and Apple caused a firestorm of legal analysis among privacy advocates and anti-terrorism groups.

Apple continues to defend the position of privacy for its customers, while the FBI seeks to compel Apple to change the configuration of its products by building a custom version of iOS software that allows the FBI to unlock the phone. Apple refused to build another version of software, maintaining that the highly secure locking mechanism was a feature of its iPhone product. The FBI eventually dropped the case against Apple after hiring an organization, which successfully hacked into the phone of the San Bernardino, California terrorist. Apple upholds its responsibility of securing the phones from external hacking and providing customers with data privacy (Hollister & Guglielmo, 2016).

CHAPTER 3

METHODOLOGY

The credit market continued to focus on PIN validation until the disruption of the Apple iPhone for contactless payment was accepted by consumers. ATM fraud, such as card skimming, rose 546% from 2014 to 2015, resulting in losses estimated as high as $2 billion (Williams, 2016). Consumer demands for contactless payments without compromising financial account security have increased in the retail industry (Green, Whitehead, & Hardie, 2017). Biometric credit cards remove the need for a PIN and provide the consumers with contactless card capabilities and enhanced security. The purpose of this study was to determine if a biometric credit card would provide higher authenticity identity proofing during a credit card transaction, resulting in fewer incidents of lost/stolen credit card fraud when compared with 2016 lost/stolen fraud rates. The study conducted was a mixed methods approach to an experimental study. The first phase of the study was the biometric card experimentation. Through the actual registration and purchase with the biometric cards, participants were given the opportunity to both successfully use their registered biometric card and attempt a purchase on someone else's card. The attempted purchase of an invalid card, representing a lost/stolen card, was considered a direct attack of credit card fraud.

The second phase of the study was a measurement of the consumer perceptions of biometric credit cards in relation to fraud occurrences through the use of a survey. In addition to the biometric card registration, the same participant group will complete the survey instrument. Each phase of the study could be analyzed separately. However, the mixed methods approach postulates the potential viability of the biometric card.

Population and Sample

The population used was a convenience sample of 200 participants chosen from two different shopping centers in the Commonwealth of Virginia. These shopping centers were chosen to represent the population that uses physical cards to make purchases in traditional brick and mortar retail stores. While biometric credit cards are contactless, to test the card's biometric capability as a means of identity proofing, a physical card with an in-store purchase is necessary. The author used the same set of participants for the experiment and the survey instrument. The selection of 200 participants sufficiently provided for 200 accounts of attempted fraud transactions, 200 accounts of attempted legitimate purchases, and 200 evaluations of consumer perceptions. Participants were only limited to persons, ages 18 and older, who had at least one fingerprint.

Biometric Card Instrumentation

The biometric credit card used for this study was a replica of the actual card used in production by Mastercard, Gemalto, and Bank of Cypress. The users' fingerprints are registered directly onto the card and stored only within the credit card. No external database stored any of the biometric data. Each biometric credit card was registered to a single user. In addition to the biometric card, a contactless terminal was used for the initial registration. The biometric credit card contained no internal batteries and used the RF-field energy harvesting power from a contactless terminal in order to register the card and create a purchase transaction. The make and model of the contactless terminals was not a determinant in this study.

The biometric card operated by using a wireless transmitter built into the biometric card, which transmitted the authorization signal of pass or fail based on the registered card's stored authorization data. When the fingerprint was pressed against the card and swiped over the terminal during a purchase, an electric output signal was distributed according to the pattern of the fingerprint. Embedded in the biometric credit card were fingerprint sensors capable of detecting and sensing the patterns contained in the fingerprint, which were used for identity proofing.

During the initial fingerprint registration process where the account holder registered his/her fingerprint to the biometric card, the fingerprint data was stored directly within the card, and no fingerprint data was sent electronically at any point during the process. The registration process was comprised of three simple steps, as follows.

Step 1: Participant placed desired finger (thumb recommended) onto the fingerprint section of the card.

Step 2: Participant waved the credit card across the contactless terminal, which provided power to the credit card.

Step 3: Fingerprint was saved directly onto credit card. No information was transmitted on the credit card terminal.

Publicly available financial data for lost/stolen credit card fraud was used for comparison to the actual data gathered during the experiment. Based on the recent production of the innovative biometric card, the lost/stolen credit card fraud data represented for 2017 is divided between biometric cards and nonbiometric cards. This division provides a direct comparison of the impacts to lost/stolen card fraud when using the biometric card.

Survey Instrumentation

The survey instrument was designed to measure the following categories: consumer perceptions of credit card fraud, ease of use of the biometric card, consumer attitudes towards risk, consumer attitudes towards identity proofing, and consumers attitudes towards privacy. The questions were divided based on these categories, but the question sequence was inconsequential and deemed to have no impact on the outcome of the responses based on the utilization of Likert scale-based questions (Weng and Cheng, 2000).

Performing the survey simultaneously with the biometric card experiment facilitated the timely capture of information while, also, providing the same participant base for both the experiment and the survey. The chances of survey participation were nearly 100%, since the survey was completed immediately following the credit card experiment. The goal of the survey was to find correlations among the categories. The survey was self-administered immediately following the successful registration of the fingerprint to the biometric credit card, a successful purchase, and an attempted fraudulent purchase.

Data Analysis Methods & Design

A convenience sample was used for both the biometric card experiment and the survey instrument in order to maximize participation and target brick and mortar shoppers. The results of the study may limit the transferability of results to other geographic locations. However, based on the cost of obtaining the biometric cards and the coordination with the registration of those cards by an industry subject matter expert, the convenience sample provided the most feasible solution for obtaining the data. The data analysis is unaffected by the convenience sample, although noted for informational purposes.

The study was guided by research questions employing quantitative analyses through the experiment followed by survey results. External reporting provided sustainable comparisons of existing successful fraud rates for the prior two years.

Research Question 1: Did the biometric-enabled device prevent a thief from using a counterfeit/lost/stolen card to make a purchase transaction?

Research question 1 was determined by measuring number of occurrences cards were effectively disabled or failed by the inability to match the user with the card and compared with the number of occurrences cards were successful in completing a transaction with a mismatching biometric identity. In addition, the study evaluated the product's capability to disable a card versus fail a card after multiple attempts and if the account hold would receive fraud alert notifications. General aggregate data was collected and reported.

Research Question 2: Did the results provide sufficient evidence for the reduction in fraud using biometric-enabled credit card device?

For research question 2, device false negatives were determined present when matching fingerprints resulted in a failed transaction at the merchant terminal. The reasons for such an occurrence vary and are not included in the data analysis. Device false positives were determined present when mismatching fingerprints are passed at the merchant terminal. These occurrences are vital to the analysis, because each occurrence is considered a successful fraud attempt. However, reasons for the occurrence, such as the percentage of minutiae due to fingerprint smudges caused by dirt or lacerations, are not determined and are not part of the data analysis. The device false positives were measured against the number of failed fraudulent transactions to determine the expected rate of fraud. These calculations were compared to the 2016 and 2017 rate of successful fraud attempts for physical credit cards of 32% for both years respectively (LexisNexis, 2017). The following variables were determined based on the formulas shown below:

2016 Fraud Rate: Number of lost/stolen fraud occurrences during 2016/Number of total fraud occurrences during 2016

2017 Fraud Rate: Number of lost/stolen fraud occurrences during 2017/Number of total fraud occurrences during 2017

Expected Biometric Card Fraud Rate = Device False Positive / (Device false positive + Number of Failed Fraudulent Transactions)

A T-test was used to compare the expected biometric card fraud rate in the experiment to the rate of successful fraud occurrences in 2017. A one-way analysis of variance (ANOVA) was used to determine if any statistically significant differences between the device false negative, device false positive, the number of failed fraudulent transactions, and the number of successful transactions. The a priori set alpha was .05. Additionally, the least significant difference (LSD) test was performed to determine the statistical significance between the means of the independent variables. The statistical analyses used were able to determine if a statistically significant relationship exists between the successful fraud rates using the biometric credit card and existing fraud rates using traditional magstripe and EMV chip cards in the current marketplace.

Research Question 3: Would the biometric-enabled device allow the consumer to maintain control over their biometric data?

No data analysis was required for research question 3. Logs were evaluated to determine if the biometric card stored any biometric data (fingerprint) within the card and whether this data was transmitted through the merchant terminal, impacting data privacy and security. The storage mechanism of the fingerprint data was determined using the manufacturer's product specifications. In order to determine the impact on data privacy, the information being passed through the authorization logs were evaluated. Any presence of biometric data being passed was acknowledged for each of the biometric test cards. Based on the construction of the biometric card, the presence of biometric data would result in inconsistencies in product specifications. This data was not used in any fraud calculations or comparisons and was presented in effort to emphasize themes concerning identity proofing and data privacy awareness.

Research Question 4: Are consumers attitudes towards biometric credit cards supportive in order to reduce credit card fraud?

In addition to the results of the physical biometric card experiment, the consumer perception of fraud and the biometric card is important to explore the themes and issues to be addressed by financial institutions seeking to utilize biometric credit cards as a future product. The use of closed questions, indicated by selecting a response provided by the researcher, were applied to determine categorical variables. In order to measure the consumer attitudes towards cards, the following categories were measured: attitude towards identity proofing, fraud perceptions, ease of use, and consumers' attitudes towards data privacy. These were evaluated against the following dependent variables: previous positive fraud experience, age category, credit card ownership, and the corresponding biometric card device false positive result for the participant.

A three-way ANOVA was used to determine the relationship between previous fraud experience, age, and the biometric card device false positive result from the experiment to the consumers' attitudes towards identity proofing, fraud perception, and ease of use of the biometric card. Additionally, descriptive statistics were analyzed, comparing the ease of use scores to the participants' age. Age was evaluated for statistical significance in ease of use and the perceived reduction of fraud.

Each of these data points provided quantitative evidence of the viability of biometric credit cards to provide high authenticity identity proofing and the expected future impact on the rate of successful credit card fraud transactions for lost/stolen physical cards. Additionally, the data provides statistical evaluation of the consumers' perceptions of fraud and prospective use of biometric cards.

CHAPTER 4

DATA ANALYSIS

Overview

The purpose of this chapter is to report the results of the data collected and the statistical analyses performed against each of the research questions. Included is a description of the data extracted for each of the instruments, the outcomes of each of the tests, and a summary of key research findings. Descriptive data, fault analysis, and statistical reports are provided in support of the analysis.

The research instruments were comprised of two separate components, the biometric credit card and the survey. Both instruments were distributed jointly as part of the experiment. From the experiment, 200 responses were collected for both instruments. A successful collection was considered a participant who attempted to register his/her fingerprint on the biometric card and completed the survey. Unsuccessful card registrations were included in the data collection for analysis and the corresponding survey noted the unsuccessful registration. The purpose of this linkage was to determine if survey results were significantly different for those who experienced problems when registering the biometric card from those who were able to register successfully.

The biometric credit card was registered on-site to 200 random participants to determine the rate of fraud and the viability of a biometric credit card for verifying proof of identity. The results of fraud occurrence found during the study were evaluated against 2016 and 2017 physical card fraud rates. Additionally, the survey was used to measure the attitudes towards biometrics as a means of credit card fraud reduction and towards personal privacy. Utilizing this method of data gathering provided a 100% response rate on the survey instrument.

Five participants were unable to register the fingerprint onto the biometric credit card successfully, and seven additional participants were unable to make a purchase using their registered biometric card on the first attempt. There were three successful attempts to make a fraudulent purchase, a sharp contrast to the 2016 and 2017 rates of 32% physical card fraud.

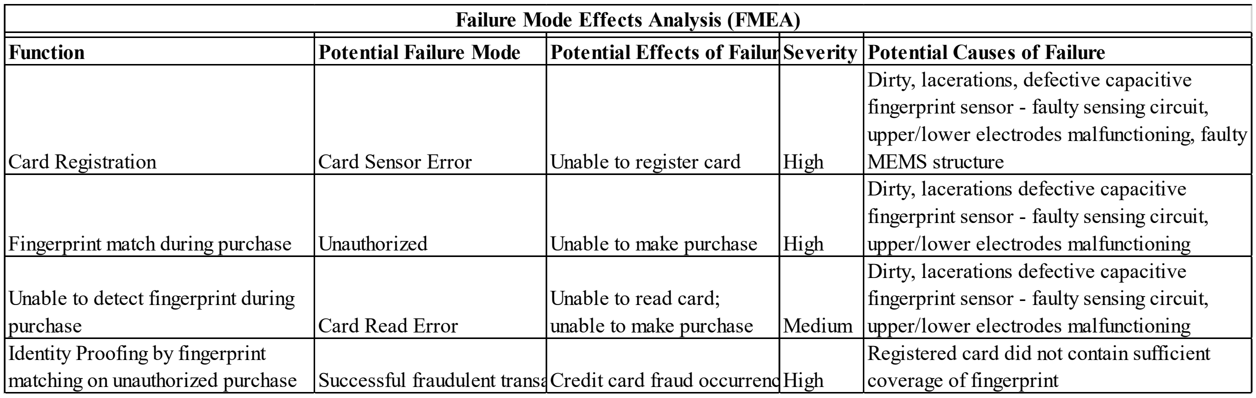
Failure Mode Effects Analysis

A Failure Mode Effects Analysis (FMEA) was performed for unsuccessful registrations or purchases to establish the cause of the errors. Errors could result from dirty fingers, lacerations, defective capacitive fingerprint sensors, faulty sensing circuit, upper/lower electrodes malfunctioning, or faulty MEMS structure. The impacts of these errors could cause a participant to be unable to register the card, make a purchase, or allow for a fraudulent transaction.

Based on Table 5, the Failure Mode Effects Analysis indicates potential points of failure during each of the functions necessary for successful usage of a biometric credit card. Four functions were identified along with corresponding failure modes along with causes and effects of the failure. An example is the card sensor error, which prevents the fingerprint from being recorded into the MEMS chip resulting in cards that are unable to be registered. Other functions analyzed were: fingerprint detection and fingerprint matching during a purchase, or encountering a successful fraud attempt.

Table 5

Failure Mode Effects Analysis by Function



Failure Mode Effects Analysis (FMEA)				
Function	**Potential Failure Mode**	**Potential Effects of Failur**	**Severity**	**Potential Causes of Failure**
Card Registration	Card Sensor Error	Unable to register card	High	Dirty, lacerations, defective capacitive fingerprint sensor - faulty sensing circuit, upper/lower electrodes malfunctioning, faulty MEMS structure
Fingerprint match during purchase	Unauthorized	Unable to make purchase	High	Dirty, lacerations defective capacitive fingerprint sensor - faulty sensing circuit, upper/lower electrodes malfunctioning
Unable to detect fingerprint during purchase	Card Read Error	Unable to read card; unable to make purchase	Medium	Dirty, lacerations defective capacitive fingerprint sensor - faulty sensing circuit, upper/lower electrodes malfunctioning
Identity Proofing by fingerprint matching on unauthorized purchase	Successful fraudulent transa	Credit card fraud occurrenc	High	Registered card did not contain sufficient coverage of fingerprint

Four probable failure modes are categorized as follows on Figure 7: materials, method, MEMS chip, and print quality. The importance of acknowledging the modes and effects of the failure provide clarification on the cause of false negative and false positive results, as well as errors that occurred during the study. For cards that were unable to be registered or card purchases that could not be authorized, card sensor errors were received due to numerous potential failure modes. Other causes were defective capacitive fingerprint sensors, faulty sensing circuit, upper/lower electrodes malfunctioning, or faulty MEMS structure. Successful fraud attempts, fingerprint matching on unauthorized purchase, could materialize if the registered card did not contain substantial coverage of the fingerprint. Additional analysis of the faulty chip is required to determine the exact cause of the successful fraud attempt.

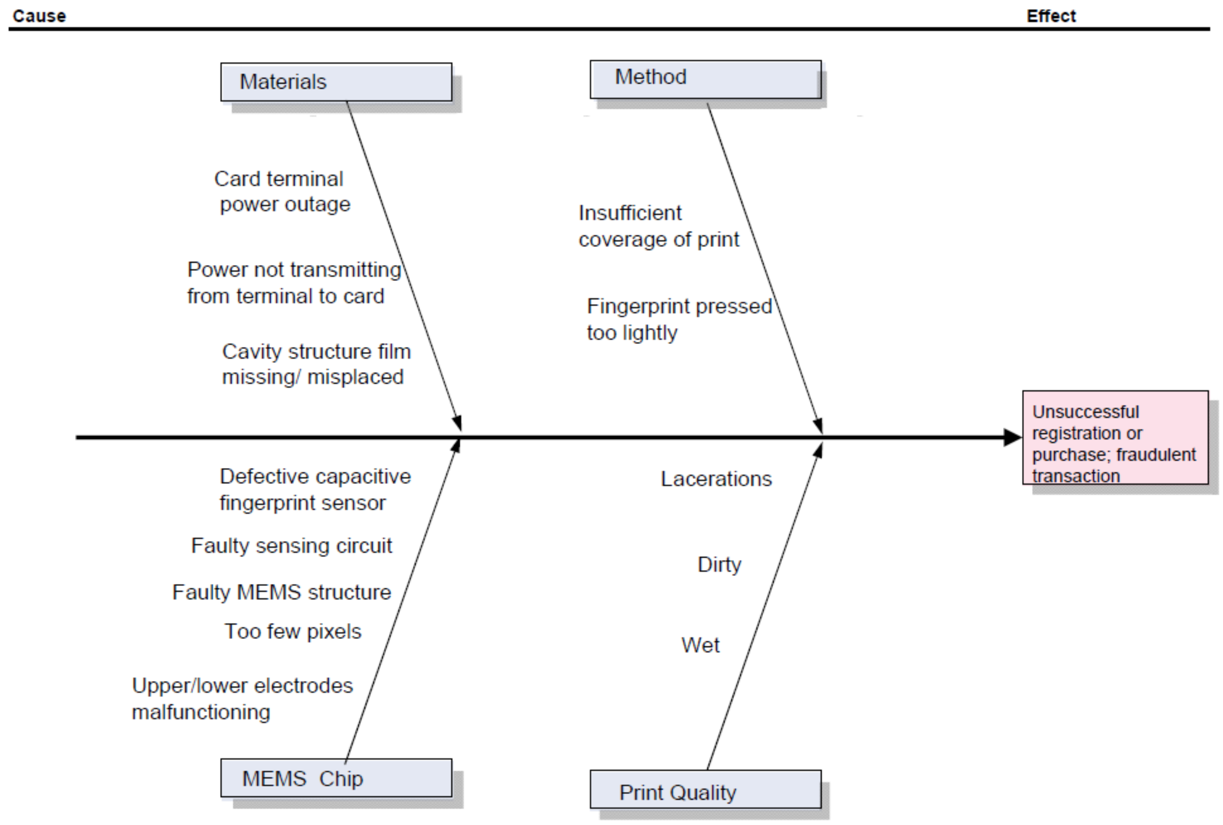

Cause
Effect
Materials
Method
Card terminal power outage
Power not transmitting from terminal to card
Cavity structure film missing/ misplaced
Insufficient coverage of print
Fingerprint pressed too lightly
Unsuccessful registration or purchase; fraudulent transaction
Defective capacitive fingerprint sensor
Faulty sensing circuit
Faulty MEMS structure
Too few pixels
Upper/lower electrodes malfunctioning
Lacerations
Dirty
Wet
MEMS Chip
Print Quality

Figure 7

Biometric Card Failure Analysis Diagram

Capacitive fingerprint sensing, as used in the biometric credit card, senses changes in the ridges and valleys to determine fingerprint pattern recognition on the sensor's surface (Tang et al., 2018). The weakness in using capacitive fingerprint identification devices is the ease in which they can be damaged due to their limited detection distance and the thin protective coating. Alternative designs have been proposed that use a glass screen to protect the fingerprint recognition sensor. Existing capacitive fingerprint sensors require high mechanical durability for installation on mobile devices and to support the elevated operating frequency.

Capacitive fingerprint sensors have a detection distance of less than 250 µm and an average protective coating of 50–100 µm on sensor-sensitive surfaces (Kyung-Hoon, Jaehuk, 2017).

To increase the accuracy rates, the fingerprint electrostatic imaging method to detect the fingerprint can be utilized and has been proposed by Tang (2018). This method has been primarily applied to fields of electrostatic protection. According to Tang (2018), "the detection distance of the sensor is 46% higher than the distance of traditional capacitive fingerprint recognition with better imaging quality". Tang's proposal of electrostatic imaging was not carried out as part of this study but could be considered in a future study to evaluate the error rate found with the false positive and false negative results.

Biometric Card Instrument, Part 1

RQ1: Did the biometric-enabled device prevent a thief from using a counterfeit/lost/stolen card to make a purchase transaction?

$RO1_1$: Determine if lost/stolen cards can be effectively disabled by the inability to match the user with the card.

The study evaluated the product's capability to disable a card after three failed purchase attempts and determine whether the account holder would receive fraud alert notifications. A disabled card is defined as a card rendered unable to use, also known as blocked. Blocked cards occur currently when financial institutions suspect fraud due to deviances from typical shopping patterns that trigger the behavior-based algorithms to yield a fraud alert. Disabled cards cannot be used again until the customer contacts the banking institution and confirms the suspicious transactions to re-enable/unblock the card and make it usable again.

The results of the study indicated that each failed purchase attempt resulted in a failed authentication message. When the user's fingerprint did not match the card, the authentication should fail. A card disabled and rendered useless after multiple failed authentication attempts would be a benefit for both financial institutions and customers. Existing fraud alert processes could be used to notify customers of the purchase attempts. Throughout the study, the failed authentication message indicated success in preventing fraud, but the cards that failed authentication up to three consecutive times were not disabled. Observations made during the transactions indicated that a card would not be disabled after three repeated attempts to make a fraudulent purchase.

While current physical credit cards can have unlimited purchase attempts until fraud alerts are triggered, most banking institutions provide safeguards to disable the card after the behavior-based algorithms determine fraud was attempted. Banking institutions can trigger these alerts on legitimate transactions, and customers are forced to call the bank and confirm their own transactions. Although cases of mistaken fraud can be an annoyance to customers, these safeguards provide an additional layer of protection to prevent a thief from continued use of a stolen credit card.

Authentication schemes have been explored to provide added security when combining biometrics with passwords. Various studies have explored biometrics-based multi-server authentication schemes, each asserting the highest levels of security. These claims have been tested and found that the schemes can be reproduced and imitated, and the authentications are at risk for denial of service attacks. Multi-server approaches have been determined insecure against forgery (Lu, 2015). Each subsequent study seeks to eliminate the vulnerabilities exposed in the authentication process.

Biometric cards do not alter the current authentication process, and any weaknesses or vulnerabilities that currently exist would remain unless efforts were undertaken to alter the authentication schemes. The EMV chip provided enhanced authentication processes but are subject to vulnerabilities. Add the biometric component will allow the biometric card to proceed with the existing authentication process but with the proof of identity already established on the card's functionality. An incorrect match renders the card useless but not disabled. The user could attempt to match the card an endless number of times. The inability to disable the card is a potential security vulnerability. While it does not violate any existing security standards, the risk is ostensible. A thief could attempt to lift the fingerprint and create a duplicate. The thief would have endless opportunities to test the result.

Fingerprint smudges on the top layer of the sensor could easily be lifted for duplication. The protective film would be expected to contain the last fingerprint of the user. While the fingerprint is validated using sensors, having copies of the ridges and patterns would be necessary for duplication efforts. Having a card that is disabled after multiple unsuccessful attempts would be an added deterrent but does not prevent a thief from stealing and attempting to replicate the print.

Performance rates of authentication can be a huge deterrent to consumers, who use cards for convenience instead of cash. The biometric card does not add any time to the transaction for identity proofing. In fact, the transactions are shorted by the time the consumer normally spends entering a PIN number, unless passwords are required as an additional mode of authentication.

RO2$_1$*: Determine if purchase transactions will fail at the credit card terminal when a lost/stolen card purchase is attempted.*

For each successful registration, a fraudulent purchase was attempted on the registered card. This process was achieved by having a participant attempt to make a purchase using a card registered to a different participant. The expected mismatch in fingerprints should have yielded a failed authentication. Of the 200 participants, 195 attempts at fraud were made based on the 195 successfully registered biometric cards. Three false positive matches passed the authentication process. The three false positive matches would have resulted in successful fraud attempts on a stolen card. The results of the study indicate that purchase transactions will fail when the user's fingerprint does not match the biometric card with a 1.5% error rate in preventing fraud. Fingerprints, when used as a single mode of authorization, have a standard 2.21 percent error rate (Moganeshwaran, Mohamed, & Suhaini, 2012). The error rate achieved with the biometric card is 0.71% lower than indicated in previous studies of biometric accuracy.

The biometric card included the EMV chip technology. However, if a card is stolen and successfully passes authentication, the chip provides no benefit in fraud prevention. Numerical PIN numbers are often not required. In such cases, the fingerprint alone acts as the PIN with no additional identity proofing required. In each of the transactions attempted during the study, no password was required. Therefore, the chip functionality added no additional consumer protection.

RO3$_1$*: Determine if fraud alerts can be triggered to the account holder after a failed attempt using the biometric-enabled device to execute a transaction.*

Authentication either approves or denies access to the system by confirming identity of the user. Only after successful authentication does the transaction proceed to authorization. Fraud alerts would be triggered only after authentication was successful, a purchase was attempted, and authorization was approved. The unsuccessful fraud attempts did not pass the authentication process and would not trigger fraud alerts, Figure 9. Because the three false positive transactions successfully passed the authentication process, fraud alerts could be triggered by a financial institution, as shown on Figure 8. Transaction logs indicated the following results:

- Successful authentications proceed to authorization and are subject to existing fraud detection models and potential fraud alerts
- Failed authentications do not proceed to authorization and would not trigger fraud detection models or fraud alerts

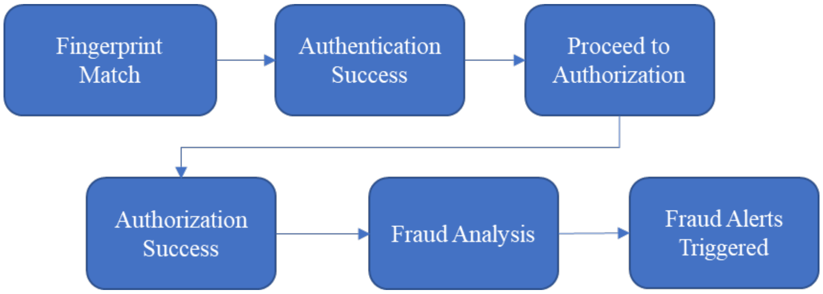


Figure 8

Biometric Card Successful Authentication

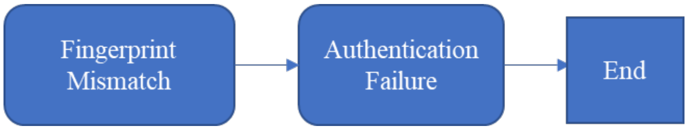


Figure 9

Biometric Card Authentication Failure

In the study results, fraud alerts could be triggered for the three successful false positive purchases using fraud detection models already implemented by the financial institutions, such as behavior-based algorithms. Existing fraud detection models would be used to evaluate the legitimate and fraudulent purchases. Whether or not the three fraudulent transactions would be identified as fraud is dependent upon the model and parameters being used in the detection models of each specific financial institution; fraud detection models were not part of this study. Based on the analysis of the biometric card, fraud alerts cannot be sent to the accountholder after a failed attempt in using the biometric-enabled device to execute a transaction, because they do not pass the authentication process. Fraud alerts are only sent after successful authentication and authorization.

RQ2: Did the results provide sufficient evidence for the reduction in fraud using biometric-enabled credit card device?

RO1$_2$: Determine the level of overall reduction in fraud when the use of a biometric-enabled device is applied prior to the user authentication process and at transaction initiation.

Based on the 200 total participants, successful registrations were received for 195. Only five were unable to be registered, four fingerprints were dirty, and two had lacerations. The

97.5% of successful registrations provided a solid number of participants for providing statistical analyses, Table 6. Each of the 195 participants with successfully registered biometric credit cards attempted a legitimate purchase on their registered card and a fraudulent purchase on a previously registered biometric card.

Analysis was not performed to determine whether materials, MEMS chip, or errors in the method of fingerprint application caused the five unsuccessful registration attempts. Such causes were noted, but only minutiae categorized as dirty, clean, or lacerations present were documented, Table 7. Additionally, the number of clean registrations, indicated by fingers that had no visible signs of dirt on the finger used for registration, made up a solid majority of the registrations (Tang, 2018).

Table 6

Biometric Card Participant Registrations

Successful Registration (Y/N)

		Frequency	*Percent*	*Cumulative Percent*
Valid	2	5	2.5	2.5
	1	195	97.5	100.0
	Total	200	100.0	

Table 7

Fingerprint Quality

Clean/Dirty/Lacerated Print

		Frequency	*Percent*	*Cumulative Percent*
Valid	C	194	97	97
	D	4	2	99
	L	2	1	100
	Total	200	100	

Particular focus on the dirty, lacerated, or undetermined prints were analyzed against the number of successful fraud attempts. All false positive results indicated a successful fraud attempt, as a biometric match was identified when the expected result was an error and unsuccessful purchase. The three false positive results, Table 8 all contained a dirty registration of the biometric credit card.

Table 8

Fraud Based on Fingerprint Quality

Successful Fraud Attempt * Clean/Dirty/Lacerated Crosstabulation

Count		*C*	*D*	*L*	*Total*
Successful Fraud Attempt (Y/N)	2	194	1	2	197
	1	0	3	0	3
Total		194	4	2	200

Throughout the experiment, the ability to successfully make a purchase using the biometric card without receiving authentication errors was evident in the 94% of participants who made purchases on the first attempt. However, as indicated on Tables 9 and 10, of the 6% of purchases that failed on the first attempt, 4% were successful on the second purchase, leaving the remaining 2% unable to make a purchase.

Table 9

Purchases Successful on First Attempt with Biometric Card

Successful Purchase 1st Attempt (Y/N)

				Valid	Cumulative
		Frequency	*Percent*	*Percent*	*Percent*
Valid	2	12	6.0	6.0	6.0
	1	188	94.0	94.0	100.0
	Total	200	100.0	100	

Table 10

Purchases Successful only on Second Attempt with Biometric Card

Successful Purchase 2nd Attempt (Y/N)

				Valid	Cumulative
		Frequency	*Percent*	*Percent*	*Percent*
Valid	n	192	96.0	96.0	96.0
	2	4	2.0	2.0	98.0
	1	4	2.0	2.0	100.0
	Total	200	100.0	100	

In order to adequately address the research question, the confidence level of the registration process and successful legitimate purchases provided sufficient evidence of the usability of the biometric card for processing through authentication and authorization processes. The key to evaluating fraud was based on the number of occurrences of false positive transactions occurring when a participant attempted to use a card registered to a different participant. Of the 200 participants, fraud was attempted on the 195 successfully registered cards.

The three successful occurrences of fraud constituted 1.5% of overall fraud, Table 11, in comparison to the 2016 and 2017 fraud percentages of 32% for each year. The stark reduction in successful fraud attempts indicates that utilizing biometrics as a form of identity proofing will likely reduce the number of fraud occurrences using physical credit cards for transactions.

Table 11

Percentage of Successful Fraudulent Transactions

Successful Fraud Attempt (Y/N)

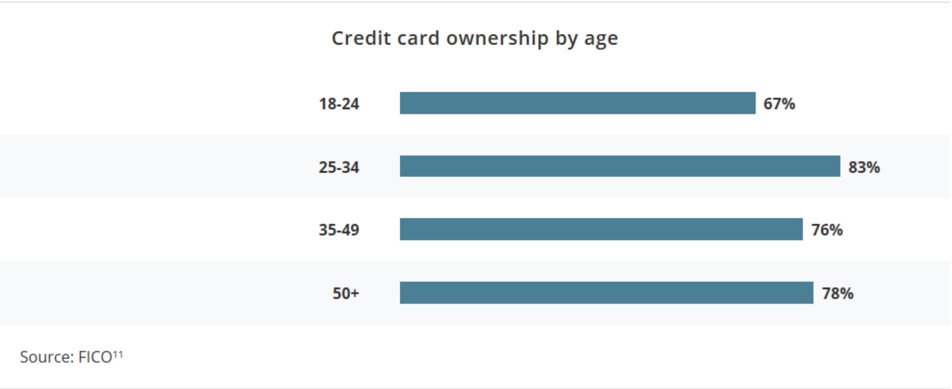
		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	No	197	98.5	98.5	98.5
	Yes	3	1.5	1.5	100.0
Total		200	100.0	100	

Successful Registrations	*False Negatives 1st Attempt*	*False Negatives 2nd Attempt*
195	7	3

RO2$_2$: Evaluate the percentage of the marketplace expected to utilize the biometric-enabled device.

Using the survey instrument, question 2.8 addresses the attitude towards consumer's comfort level using a biometric credit card. The question states, "As a consumer, I feel comfortable providing my fingerprint at a point of sale terminal in order to validate that I am an account holder." Based on the number of credit card owners shown in Figure 10 by Fair Isaac Corporation, the largest group of credit card owners are those aged 25-34. However, the majority of adults owned credit cards regardless of age category. In the study, the largest number of participants were ages 35-44, Table 12. Overwhelmingly, participants felt comfortable providing a fingerprint as a form of identity proofing at a point of sale terminal. As indicated in Table 13, those who agreed accounted for 57% and strongly agreed were 29%. Cumulative, this is 86% of participants who feel comfortable providing their fingerprint to validate their identity in a transaction.

Survey results were not significantly different for those who experienced problems when registering the biometric card from those who were able to register successfully. The number of unsuccessful registrations were not numerous enough to determine statistical significance from the population sample provided. Responses differed minimally based on the biometric card experience. For the participants who were able to successfully trigger a fraudulent transaction, the confidence of the biometric card was reduced. Regardless of this result, the attitude towards using biometrics was not largely different from participants who were unable to complete the fraudulent purchase successfully.



Source: FICO[11]

Figure 10

Fair Isaac Corporation: Percentage of Credit Card Owners by Age

Table 12

Participants by Age Category

Age Category

		Percent
Valid	18-24	28.6
	25-34	14.3
	35-44	42.9
	45-54	14.3
Total		100.0

Table 13

Perception of Reduction in Fraud Using Biometrics for Identity Proofing

Biometric Decreases Fraud

		Valid Percent
Valid	Disagree	14.3
	Agree	57.1
	Strongly Agree	28.6
Total		

RO3$_2$: Evaluate the current levels of fraud related to physical credit card devices.

Fraud rates for 2016 and 2017 for physical credit cards based on lost and stolen cards were 32% respectively for both years based on LexisNexis reports. The study performed by LexisNexis evaluating the true cost of fraud for 2016 found that “retail fraud continues to rise dramatically as does its cost. The level of fraud as a percentage of revenues has also inched upwards (1.32% to 1.47%)” (pp. 5). The cost of managing fraud continues to rise, and fraud detection models are not fully automated. Roughly half of potentially fraudulent transactions flagged by the algorithms are manually reviewed, driving up the costs for fraud prevention.

Furthermore, transactions erroneously flagged as fraud are increasing due to the utilization of multiple fraud management tools. Whether the reduction in fraud is a selling point for the financial institutions as well as the merchants is discouraged by the cost of managing fraud (LexisNexis, 2016).

The results of the study provide evidence of the capability of achieving credit card fraud reduction at a minimal cost. Based on the estimated cost of manufacturing, processing, and delivering the biometric credit card at an average cost of $3.00 per card compared the EMV chip card cost of $2.25, the additional $0.75 may be worth the cost for financial institutions in exchange for potentially fewer flagged transactions. Comparing the 2016 and 2017 physical card fraud rates of 32% to the 1.5% biometric card 'error rate' in preventing fraud, the benefits may outweigh the cost.

RQ3: Would the biometric-enabled device allow the consumer to maintain control over their biometric data?

RO1$_3$*: Determine if the biometric-enabled device will store the biometric data (fingerprint) within the card and will not transmit the data through the merchant terminal, providing privacy and security.*

Consumers wishing to retain control over their biometric data are generally assumed to be opposed to allowing biometric data to be stored electronically by a private or public institution. Privacy of PII data remains a concern of consumers with higher levels of protection desired for biometric data. The study targeted the data passed through the authentication and authorization process. Whether biometric data was stored within a receiving system or transmitted as part of the purchase transaction was measured by monitoring the logs for any activity representing the biometric type data from the merchant terminal. The results indicated no biometric data was passed or evaluated within the financial institution’s system. The biometric card stored the fingerprint directly on the card but did not transmit the data from the card to the terminal.

RO2$_3$: Define the storage mechanism of the fingerprint data.

As part of the card registration process, a small modular unit, also known as an IDEX remote enrollment sleeve, was used to provide the capability to capture the fingerprint without going to a banking institution for recorded digital prints. The participants placed their fingers onto the fingerprint scanner, located on the biometric card, three times until the fingerprint was recorded successfully. Though five unsuccessful registrations occurred, the study did not include an evaluation of the algorithms used to store the fingerprint data to determine the cause of the errors. Each fingerprint was stored as an encrypted template of numbers. No physical images were recorded electronically nor was any data passed systematically to the Internet.

Biometric Card Survey Instrument - Part 2

RQ4: Are consumers attitudes towards biometric credit cards supportive in order to reduce credit card fraud?

Categorical questions were included in the survey instrument, Appendix A, in order to gain the consumer’s perspectives on fraud, biometrics, privacy, and corporate responsibility. Participants were asked to designate a score for each question based on the levels 1-5, as follows: 1 – mostly disagree, 2 – disagree, 3 – neutral, 4 – agree, and 5 – mostly agree.

Additional demographic data, such as gender and nationality, was captured to determine a relationship to age and previous fraud victims.

RO4$_1$: Evaluate the consumers' attitudes towards corporate responsibility in reducing fraud.

A multivariate analysis of variance (MANOVA) test was performed to evaluate the relationships between age, victims of fraud, attitudes towards credit card bank selection based on a company's ability to combat fraud, and attitudes towards recommending that companies use biometrics as a means of identity proofing for preventing fraud. The solid distribution between age categories and fraud victims, as shown in Table 15, allowed for an analysis by each age group and victim category. In order to execute the multivariate analysis, the data was checked to ensure the data met the conditions for the MANOVA. In addition to verifying the age distributions, a Q-plot (Figure 11) was executed to determine the linear relationship between those who experienced fraud and the belief that using biometrics to prove identity during transactions will deter thieves.

Table 14

Participants by Age and Victims of Fraud

Between-Subjects Factors

	Value	*N*
Age Category	18-24	44
	25-34	49
	35-44	63
	45-54	25
	55+	19
Fraud Victim	Yes	108
	No	92

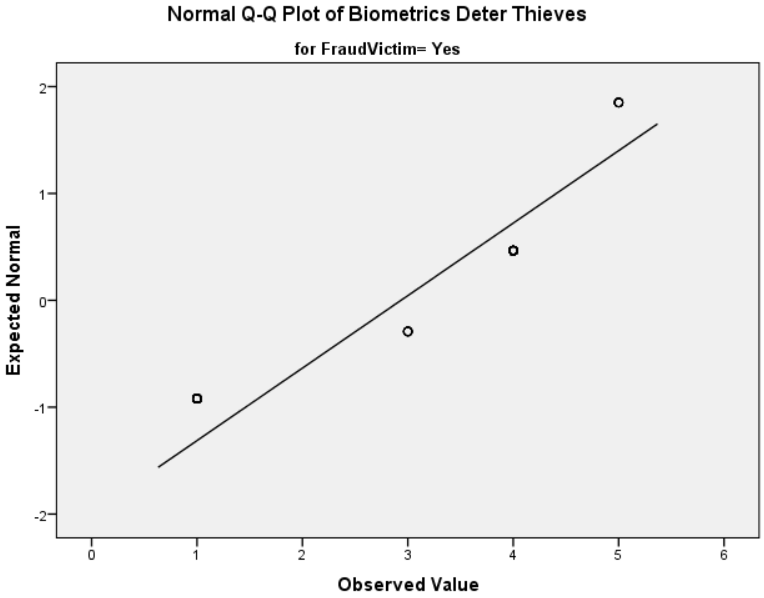


Figure 11

Linear Relationship of Fraud Victims and Attitude Towards Biometrics

Further analysis through Box's test of equality of covariance proves statistical significance of age and victims of fraud with corporate responsibility for fraud prevention and utilizing biometrics. Levene's test, Table 15, supports the results of Box's test with statistically significant results. As shown in Table 16, ages 18-24 and 45-54 had the highest scores of Agree to Strongly Agree that fraud prevention tactics by a company were crucial in selecting a bank. Table 17 provides the means for each age group based on those who had been victims of credit card fraud and those who had not. Regardless of fraud victimization, the outcomes of the analysis postulate that a bank's ability to prevent fraud is important in the selection of a financial institution for obtaining a credit card. However, the lack of a statistical relationship between age and selection of a financial institution rules out any predictive relationship. The overall results remain an indicator that nearly all age groups found fraud prevention a consideration in credit card company selection.

Table 15

Levene’s Statistical Error Variance

Levene's Test of Equality of Error Variances[a]

	F	*df1*	*df2*	*Sig.*
Bank Selection	35.979	9	190	0.000
Recommend to Use Biometrics	22.532	9	190	0.000

Tests the null hypothesis that the error variance of the dependent variable is equal across groups.

a. Design: Intercept + Age Category + Fraud Victim + Age Category * Fraud Victim

Table 16

Fraud Prevention Tools and Impact on Bank Selection by Age Category

Bank Selection

Age Category	*N*	*Subset 1*	*Subset 2*	*Subset 3*
25-34	49	3.1224		
55+	19	3.3158		
35-44	63		3.6190	
18-24	44			4.1364
45-54	25			4.2800
Sig.	Total	0.255	1.000	0.5580

Means for groups in homogeneous subsets. Based on observed means.
The error term is Mean Sample Size = 32.973
The group sizes are unequal. The harmonic mean of the group sizes is used.
Type I levels are not guaranteed.

Table 17

Age and Fraud Victim Attitudes Towards Corporate Responsibility and Use of Biometrics

Age Category * Fraud Victim

Dependent Variable	*Age Category*	*Fraud Victim*	*Mean*	*Std. Error*	*95% Confidence Interval Lower Bound*	*95% Confidence Interval Upper Bound*
Bank Selection	18-24	Yes	4.000	0.076	3.851	4.149
		No	4.333	0.091	4.154	4.513
	25-34	Yes	3.500	0.112	3.280	3.72
		No	3.000	0.064	2.875	3.125
	35-44	Yes	3.864	0.058	3.749	3.979
		No	3.053	0.089	2.878	3.227
	45-54	Yes	4.538	0.107	4.327	4.750
		No	4.000	0.112	3.780	4.220
	55+	Yes	3.000	0.107	2.789	3.211
		No	4.000	0.158	3.689	4.311
Recommended Use Biometrics	18-24	Yes	3.000	0.087	2.828	3.172
		No	4.000	0.105	3.793	4.207
	25-34	Yes	3.000	0.128	2.747	3.253
		No	3.000	0.073	2.856	3.144
	35-44	Yes	3.114	0.067	2.981	3.246
		No	2.684	0.102	2.483	2.885
	45-54	Yes	4.000	0.123	3.757	4.243
		No	4.555	0.128	4.247	4.753
	55+	Yes	2.000	0.123	1.757	2.243
		No	3.000	0.181	2.642	3.358

RO2$_4$: Evaluate the consumers' attitudes towards using a biometric credit card for purchases.

A linear regression analysis was performed to evaluate the relationship between age and fraud victim's belief that fraud is a growing problem. The regression analysis on Table 18 indicates statistical significance based on the p value of .000 and is strengthened for fraud victims. The linear regression supports the position that fraud victims are more likely to believe that fraud is a growing problem.

Table 18

Linear Regression Statistical Analysis of Fraud as a Growing Problem

ANOVA[a]

Model		*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig.*
1	Regression	6.287	2	3.143	10.920	.000[b]
	Residual	56.708	197	0.288		
	Total	62.995	199			

a. Dependent Variable: Fraud is a Growing Problem

b. Predictors: Fraud Victim, Age Category

Relationship of Fraud as a Growing Problem by Age and Fraud Victim

Model		*Coefficients*	*Standardized Coefficients*		
		Std. Error	*Beta*	*t*	*Sig.*
1	Constant	0.152		30.145	0.000
	Age Category	0.031	0.1120	1.646	0.101
	Fraud Victim	0.077	-0.282	-4.138	0.000

Dependent Variable: Fraud is a Growing Problem

A multilinear regression analysis was performed to determine if there is a relationship between victims of fraud and belief that fraud is a growing problem towards attitude towards using biometrics for identity proof during credit card purchases. The relationships were signified in an equation based on the following variables found on Table 19:

Y = The utilization of a fingerprint at a POS terminal to validate a transaction decreases the ability for a criminal to make a purchase on a stolen card.

X_1 = Victim of credit card fraud

X_2 = Belief that fraud is a growing problem

Y = (.700)Fraud Victim + (-1.5)Fraud is a growing problem + 9.1

R Square = .867

Standard Error of the Estimate = .44721

Table 19

Predictor Analysis of Fraud as a Growing Problem

Predictor Relationship of Fraud as a Growing Problem

Model	*R*	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	0.931	0.867	0.800	0.44721

Predictors: Fraud is a Growing Problem, Fraud Victim

Table 20

Predictor Analysis of Fraud as a Growing Problem by Biometric as a Deterrent

Relationship of Fraud as a Growing Problem by Biometric as a Deterrent

Model		*Coefficients Std. Error*	*Standardized Coefficients Beta*	*t*	*Sig.*
1	Constant	9.100		6.672	0.003
	Fraud Victim	0.700	0.3420	1.871	0.135
	Fraud is a Growing Problem	-1.500	-0.866	-4.743	0.009

Dependent Variable: Biometrics Decreases Fraud

A linear regression analysis was then run to analyze only the relationship between fraud victims and attitudes towards using biometrics for identity proof during credit card purchases. The relationship between those who think fraud is a growing problem to biometrics as a deterrent is statistically significant based on the calculations shown on Table 20. Removing the variable fraud victim allows for more targeted calculations to determine if a predictor relationship exist. The R square for fraud victims is not high enough to substantiate a predictor relationship.

Y = (.700)Fraud Victim + 3.100

R Square = .117

Standard Error of the Estimate = 1.02956

Table 21

Linear Analysis of Fraud Victim on Biometrics as Fraud Deterrent

Predictor Relationship for Biometrics as a Fraud Deterrent

Model	*R*	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	0.342	0.117	-0.600	1.02956

Predictor: Fraud Victim

Relationship of Fraud Victims to Use of Biometrics to Decrease Fraud

			Standardized		
		Coefficients	*Coefficients*		
Model		*Std. Error*	*Beta*	*t*	*Sig.*
1	Constant	1.174		2.641	0.046
	Fraud Victim	0.861	0.342	0.813	0.453

Dependent Variable: Biometrics Decreases Fraud

The standard error of the estimate is .44721 when considering both fraud victims and the belief that fraud is a growing problem compared to just fraud victims at 1.02956. However, the R squared value is much higher using fraud as a growing problem, demonstrating a predictor relationship between the two variables. Calculations from Tables 22, 23, and 24 support the findings. Those who believe fraud is a growing problem are more likely to believe that biometrics is a viable solution.

Table 22

Fraud is a Growing Problem Relationship to Biometrics Decreases Fraud

Coefficients of Biometrics Decreases Fraud

Model		*Coefficients Std. Error*	*Standardized Coefficients Beta*	*t*	*Sig.*
1	Constant	1.563	1.5630	6.398	0.001
	Fraud is a Growing Problem	0.387	-0.866	-3.873	0.012

Predictor Relationship for Fraud is a Growing Problem

Model	*R*	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	0.866	0.750	0.700	0.54772

Predictors: Fraud is a Growing Problem

Y = (-1.5)Fraud is a growing problem +10

R Square = .750

Standard Error of the Estimate = .54772

Table 23

R Square Analysis

	Fraud Victim + Fraud is a Growing Problem	**Fraud is a Growing Problem**	**Fraud Victim**
R Square	.867	.750	.117
Standard Error of the Estimate	.44721	.54772	1.02956

Table 24

Pearson Correlation

Pearson Correlation Matrix	**Biometric Decreases Fraud**	**Fraud is a Growing Problem**
Biometric Decreases Fraud	1.00	.866
Fraud is a Growing Problem	.866	1.00
Fraud Victim	.342	0.00

Survey results indicated that more than half of respondents had experienced some form of credit card fraud. However, recommendations to use biometrics as a means for fraud prevention remained neutral, eliminating a causal relationship between the two variables. Age was a significant factor in relation to biometrics as an invasion of privacy. Participants over the age of 45 had privacy concerns on the collection of biometric data, though they felt that fraud was a growing problem and the requirement of a fingerprint would lead to reduced numbers of fraud occurrence.

Three false positives out of 195 successful registration yields a result of 1.5% likelihood of fraud. Further analysis of the reasons for the false positives could be used to implement changes to the card sensors to increase the reliability and quality of the biometric credit card. Using the results from the study, the biometric card yielded a reduction in fraud of 30.5% of physical credit card fraud. The figures are limited to physical credit card fraud and do not consider online or mobile fraud attempts.

Device false negatives were present during the study and are considered when matching fingerprints resulted in a failed transaction at the merchant terminal. Seven of the 195 registered cards received a false negative match when attempting to make a purchase. In each of these cases, the user of the card was the same person who registered the card. The fingerprint should have matched. In each of the seven cases shown on Table 25, a second attempt was made to purchase on the terminal. After the second attempt, four were successful, and the remaining three rendered a second false negative result.

The causes for this discrepancy were not analyzed, and the fingerprints were considered clean, lacking any visible dirt or lacerations to the finger. The percentage of false negatives against registered cards was a total of 7 cards of 195, or 3.6%. The 3.6% of essentially unusable cards could be a large enough number to cause consumers to reject the viability of the card. Add this to the 2.5% of participants who were unable to register the card, and this leaves 12 total participants of 200, 6% of the participants who were unable to use the biometric card.

Concerns over personal privacy were addressed as part of the survey, and overall, participants did not feel that a biometric credit card violated their privacy. Table 25 provides the mean values for privacy and risk based on age group. The 35-44 age group were neutral on privacy, and the age categories of 18-24, 25-34, and 45-54 equally disagreed on the question addressing “requiring biometric fingerprint data is invasive and violates the right to privacy”. While ages 35-44 were neutral on privacy, they disagreed that risks involved in providing fingerprint data are less than the risks of fraud. The 45-54 age group felt different and agreed that risks of using biometric data were less than the risk of fraud. The younger group, from 18-34 were neutral, indicating they did not believe the biometrics were any riskier than existing chances of fraud.

Table 25

Privacy Concerns and Risks

Mean Values

Age Category		*Biometrics Violate Privacy*	*Biometrics Result in Less Fraud*
18-24	Mean Values	2.0000	3.0000
	N	2	2
	Std. Deviation	0.0000	0.0000
25-34	Mean Values	2.0000	3.0000
	N	1	1
	Std. Deviation	.	.
35-44	Mean Values	3.0000	2.0000
	N	3	3
	Std. Deviation	1.0000	1.0000
45-54	Mean Values	2.0000	4.0000
	N	1	1
	Std. Deviation	.	.
Total	Mean Values	2.4286	2.7143
	N	7	7
	Std. Deviation	0.78680	0.9512

In order to evaluate the question of difficulty in using biometrics, the researcher administered the survey after the biometric card registration and purchase were completed. This allowed the user to have an opportunity to try a biometric card rather than completing a survey without experience. While this provided more of an evaluation of the user's experience, it does not address the perceptions of difficulty by consumers who have never been exposed to using biometrics. The value in the survey question is high in its relationship to the overall biometric card study experience and should be considered in evaluations for practical use.

Nearly unanimously, respondents believe that biometric cards are easy and safe to use for making a purchase transaction. However, as can be seen in Table 26, respondents were not as agreeable to requiring biometric data as part of a credit card application. The resistance was not in providing biometric data but more focused on capturing the biometrics during the application process. In this study, no credit card application was required in order to register and use the card.

The majority of the participants responded in disagreement that requiring the biometric print during the application process would be too cumbersome. Recognizing the user's perception of the level of difficulty using the biometric card is essential to determine the influence between the user's perception and the marketability of the card. As a sample population of credit card holders, the level of resistance to using credit cards based on any complexity with capturing fingerprints seems minimal in impact. Organizations can, however, focus on reducing the impact to card holders by developing a seamless registration process and potentially utilizing devices that allow consumers to register cards from their own homes.

Table 26

Biometric Credit Card Ease of Use

Mean Values

Age Category		*Biometrics too Cumbersome*	*Biometrics are Easy and Safe*
18-24	Mean Values	2.5000	4.0000
	N	2	2
	Std. Deviation	0.7071	0.0000
25-34	Mean Values	2.0000	4.0000
	N	1	1
	Std. Deviation	.	.
35-44	Mean Values	3.0000	4.0000
	N	3	3
	Std. Deviation	1.0000	0.0000
45-54	Mean Values	2.0000	4.0000
	N	1	1
	Std. Deviation	.	.
Total	Mean Values	2.5714	4.1429
	N	7	7
	Std. Deviation	0.78680	0.0000

An important consideration for this study was the perception of biometrics in reducing fraud and as a means for identity proofing. Participant reaction to the biometric card through observation was positive and eager. Table 27 below provides evidence of the support for using biometrics to reduce fraud. All ages agree in its usage for combating fraud and an even higher average believed biometrics should be used as proof of identity. The study confirms Computer Weekly's report that "Shoppers are becoming more comfortable with paying via biometrics" (2016). Its study found that 63% of consumers want to be able to use biometric scans to authenticate payments when shopping, and 69% said they would be most open to using their fingerprints" (McDonald, 2017). Consumers' attitudes towards biometric credit cards are supportive in order to reduce credit card fraud based on the study's results.

Table 27

Mean Values by Age for Identity Proofing and Decrease in Fraud

Mean Values

Age Category		Biometric Decreases Fraud	Biometrics as a Means of Identity Proofing
18-24	Mean Values	4.0000	4.0000
	N	2	2
	Std. Deviation	0.0000	0.0000
25-34	Mean Values	4.0000	4.0000
	N	1	1
	Std. Deviation	.	.
35-44	Mean Values	4.0000	4.0000
	N	3	3
	Std. Deviation	1.73205	0.57735
45-54	Mean Values	4.0000	4.0000
	N	1	1
	Std. Deviation	.	.
Total	Mean Values	4.0000	4.1429
	N	7	7
	Std. Deviation	1.00000	0.37796

Summary

This chapter provided analysis of the findings for both the biometric card fraud prevention and consumer attitudes towards biometrics. Data was gathered in two parts with the first focused on the biometric card and addressed research questions one through three for determining level of fraud reduction, impact on fraud alerts, and privacy concerns. The second part required the survey instrument for gathering quantitative data on the consumer's willingness to use biometrics when making credit card purchases.

Part one's findings indicated successful biometric card registrations and purchases with only five cards that did not register successfully. The results exposed an error rate for the biometric card that could be used for fraudulent purposes. The biometric card did not send biometric PII data through the system and was contained for providing authentication directly through the card proper, addressing privacy concerns as well as potential storage problems for companies. Finally, the fraud alerts were found not to be triggered when a consumer tried to use someone else's card.

The second part of the study provided evidence of consumer's acceptance of the biometric credit card. In general, consumers feel that fraud is a growing problem and believe that using biometrics will result in credit card fraud reduction. Biometric cards were found to be easy to use and more secure than current means of authentication. Numerous statistical analyses were performed to determine the relationship between fraud victims and biometrics as well as age and biometrics. Linear regression analyses were performed as well as a multivariate analysis to determine predictability associations.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

The purpose of this study was to determine the level of reduction in fraud pertaining to lost/stolen/physical cards when utilizing credit cards with embedded fingerprints for identity proofing. The viability of the biometric credit was further analyzed by exploring the perceptions and attitudes of consumers towards using biometrics for identity proofing during a credit card transaction. Prior to this study, little documentation existed that examined potential fraud reduction and viability of biometrics for everyday use in making credit card purchases at merchants and the potential acceptance of this method by the general consumer population. The analyses established that strong evidence exists for using biometrics in exchange or in conjunction with the current PIN and/or signature method. Consumers agree that fraud is a growing problem. Credit card institutions' methods for handling fraud is a security issue that consumers are using when selecting a credit card company.

Additional concerns surrounded biometric data privacy, data storage, and the impact on fraud alerts triggered by the financial institution. Random participants were used for this study of various age groups of 18 years and older in order to obtain a population sample of credit card users. A total of 200 participants completed the study, resulting in 195 successful biometric card registrations. Each registered card was used for a legitimate purchase matching the registrant's card with the user's fingerprint, and for an attempted fraudulent purchase matching the user's fingerprint with a previous registrant's card. This allowed for testing of the following processes: biometric card registration, consumer purchases, fraud attempts. Results of the study indicated significant reductions in fraud based on the 2016 and 2017 fraud rates for lost or stolen credit cards. Merchant responsibility is removed as card users are able to provide proof of identity without requiring verification from the merchant through alternative ID checks.

Biometric cards were found to have a 1.5% error rate, which was determined through attempted fraudulent purchases of the registered biometric cards. The three false positives were indication of fraud attempts and measured out of 195 successful registrations. This error rate is less than fingerprint scan error rates identified in other studies. If the 32% of fraud were lost or stolen cards, and this could be reduced to 1.5% based on biometric identity proofing, the result could be significant savings in fraud for both consumers and corporations.

The capability to disable the card was not present on the biometric cards used in the study. A user could attempt to use the card repeatedly with failures, but the card was not disabled. Furthermore, the banking institution did not receive any notification of the repeated attempted use in order to perform action against the card, i.e. fraud alert. Until the fingerprint matched the card, the card is essentially not activated, leaving no reason to disable the card. In the event of fraudulent use, fraud alerts were not sent for failed authentications. Fraud alerts would only be triggered for successfully authenticated and authorized transactions using current fraud detection models.

Biometric data is personally identifiable information and raises privacy as well as data security concerns. The study confirmed that biometric data was not passed through the transaction logs during any part of the credit card transaction process. Biometric fingerprint data was only stored within the credit card.

The survey conducted gathered data for understanding consumers' attitudes towards fraud and using biometrics to combat fraud. The study was further evaluated based on age group and consumers who had or had not experience credit card fraud. Fraud victims believe fraud is a growing problem and are more likely to believe that biometrics should be used to combat fraud.

Consumer perceptions were measured based on age category for fraud prevention tactics. Ages 18-24 and 45-54 had the highest scores of Agree to Strongly Agree that fraud prevention tactics by a company were crucial in selecting a bank. Those who believe fraud is a growing problem believe biometrics reduce fraud. Little resistance to biometrics could be found, as nearly all participants responded in favor of biometrics for identity proofing and declared a biometric card as easy to use. All age groups found a company's approach to and guarantee of fraud protection and prevention important when selecting a credit card. The ease of use with the biometric card was reflective in the survey responses by the participants.

The industry demand for higher security and more credit card account protection from financial institutions is leaning towards alternative measures, and the mobile fingerprint payment method paved the way for the beginning of biometric authentication. Corporations and consumers alike benefit from increased security measures by reducing the monies spent on fraud annually. Biometrics as a form of identity proofing has existed for decades but has not been utilized by the general population. The acceptance of providing biometric data, and particularly the fingerprint, opened the opportunity for biometric card companies to manufacture cards for various purposes. The use of biometrics for identity proofing alone may not offer enough security to prevent fraudulent transactions from occurring, since the likelihood of biometric data distortion must be considered and alternative measures provided.

Limitations of Research

The survey was conducted as a joint experiment with the biometric credit card. The conjoining of these two aspects of the study did not allow for survey respondents who had never seen or experienced a biometric credit card and could have concluded differing results. Additionally, the participants in the study opted to take part based on their interest in biometrics. Those uninterested in utilizing biometric cards were more unlikely to participate, creating some level of bias. The bias created an inherent limitation to the survey results.

The location of the experiment and survey administration was the Short Pump Towne Center, located in the city of Glen Allen, Virginia. The singular location limited the study in the attitudes towards biometrics for the locality. Demographic groups were not seen as a limitation to the study when comparing ethnicities in Glen Allen to the total ethnicities in the United States of America. Based on the 2017 census, Glen Allen, Virginia is 60.5% Caucasian [60.7% nationwide], 26.8% Black [13.4% nationwide], 5.1% Asian [5.8 nationwide], 3.6% two or more races [2.7% nationwide], and 4.9% Hispanic [18.1% nationwide]. Foreign born persons represent 10.1% of the Glen Allen residents [13.2% nationwide] (United States Census Bureau, 2017).

Practical Implications

A biometric credit card that disables after multiple purchase attempts would offer added protection in excess of identity proofing. While this functionality was not available with the biometric card tested, this would be a recommendation for future card functionality. The biometric card does provide high levels of identity proofing accuracy without the disabling feature, but the additional feature could make the card more attractive for consumers.

Nearly unanimously, respondents believe that biometric cards are easy and safe to use. Identity proofing with biometrics satisfies two of the three factors: 1) something the person has – credit card; 2) something the person is – fingerprint. The third component, something the person knows, such as the PIN number, could be an additional authentication component if the financial institution chose to keep the current requirement for PIN numbers. If all three components are included, the three-factor authentication will add a layer of protection with the potential to significantly reduce fraud for lost and stolen cards.

The research suggests the biometric card would reduce fraud and be an accepted form of identity proofing for the consumer. The cost per card is a slight increase and could be passed on to cardholders. In exchange, the reduction in fraud would be a realizable return on investment. Biometric cards fill in the missing component of verifying identity by the merchant from the majority of transactions by requiring identity proofing with each purchase. As the concept of biometric credit cards become more of a reality, the data gathered and analyzed as part of this study can be leveraged by both practitioners and researchers. The data can be used to determine the viability of a biometric credit card based on cost, savings from fraud reduction, and marketability.

Future Research Recommendations

The Failure Mode Effects Analysis suggested several points of failure in the usage of a biometric credit card. Causes of failure were identified along with their impacts; however, none of the failure points were analyzed further by inspecting the individual card specifications.

Additional studies could evaluate the points of failure and determine any technical changes that need to be implemented to increase the accuracy rate of the cards. Furthermore, studies on the replication of the fingerprint from the biometric card should be pursued to determine the likelihood of card skimming. The survey instrument could be repeated with a set of individuals who have never experienced a biometric card. Results from the targeted sample could be compared to the results from this study.

REFERENCES

Bright, P. (2015, December 28). *Common payment processing protocols found to be full of flaws*. Retrieved July 3, 2016, from ARS Technica: https://arstechnica.com/information-technology/2015/12/common-payment-processing-protocols-found-to-be-full-of-flaws/

Chowdhry, A. 2014. *MasterCard And Zwipe Unveil Credit Card With Fingerprint Scanner*. Retrieved from Forbes: https://www.forbes.com/sites/amitchowdhry/2014/10/18/ mastercard-zwipe-fingerprint-sensor-credit-cards/

Clark, Nathan. *Transparent User Authentication.* (Centre for Security, Communications, and Network Research, 2011).

Fair Isaac Corporation. 2016. *FICO Decisions: The Digital Generation.* Retrieved from https://www.creditcards.com/credit-card-news/assets/FICO-the-digital-generation-are-millenials-looking.pdf

Esan, O. A., & Ngwira, S. M. *Bimodal Biometrics for Financial Infrastructure Security*. (Information Security for South Africa, 2013), 1-8.

Federal Trade Commission. (2015, November 2). *Consumer Information*. Retrieved from Protecting Against Credit Card Fraud: http://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud

Fons, M., Fons, F., & Cantó, E. *Design of an Embedded Fingerprint Matcher System.* (Tenth International Symposium on Consumer Electronics, 2006), 1-6.
Frellick, M. 2010. Retrieved from What's it cost to get a credit card in your pocket?: http://www.creditcards.com/credit-card-news/cost-getting-credit-card-in-your-pocket-1276.php

Goode Intelligence. 2015. *Biometrics for Banking; Market and Technology Analysis, Adoption Strategies and Forecasts 2015-2020*. Retrieved from http://www.goodeintelligence.com/report-store/view/biometrics-for-banking-market-technology-analysis-adoption-strategies-forecasts-20152020

Grant, K. B. (2017, February 1). *Identity theft, fraud cost consumers more than $16 billion*. Retrieved March 27, 2018, from https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html

Grassi, P. A., & Fenton, J. L. (2017, June). *Digital Identity Guidelines: Enrollment and Identity Proofing.* Retrieved November 18, 2017, from NIST Special Publication 800-63A: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

Green, A., Whitehead, E., & Hardie, S. (2017, November). *Biometrics Decrypted.* Retrieved January 29, 2018, from Zwipe: http://www.zwipe.com

Hollister, S., & Guglielmo, C. (2016, February 25). *How an iPhone became the FBI's public enemy No. 1*. CNet: http://www.cnet.com/news/apple-versus-the-fbi-why-the-lowest-priced-iphone-has-the-us-in-a-tizzy-faq/

Hong, L., Wan, Y., & Jain, A. *Fingerprint Image Enhancement: Algorithm and Performance Evaluation*. (IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998), pp. 20, 777-789.

IDCPI. (2013, May 12). *Identity Crime Prevention Institute.* Amar Singh, Operation Swiper, Queens, New York, 2011: http://www.identitycrime.org/cases/item/163-amar-singh-operation-swiper-queens-new-york-2011

Inside Arm. 2006. *Worldwide Unisys ID Fraud Study Shows New U.S. Consumer Security Concerns*. Retrieved from http://www.insidearm.com/news/00007194-worldwide-unisys-id-fraud-study-shows-new/

Kaye, D. (2003). *The Nonscience of Fingerprinting: United States v. Llera-Plaza*. Retrieved from Law Review Library: https://www.qu.edu/prebuilt/pdf/SchoolLaw/LawReviewLibrary/43_21QLR1073(2001-2003).pdf

Knieff, Ben. (2016). *2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From.* Boston, MA: Aite Group.

Kobs, K. (2015). *EMV is Here -- Is Your Business Ready?* Franchising World, 47(8), 47–48. Retrieved from https://ezproxy.indstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bah&AN=110151419&site=ehost-live&scope=site

Krishnan, A. P., & Sy, B. K. (2012). SIPPA-2.0 – Secure Information Processing with Privacy Assurance (version 2.0). *Tenth Annual International Conference on Privacy, Security and Trust*, 25-34.

Kyung-Hoon, S.; Jaehuk, C. (2017). A Method for Enhancing the Sensing Distance of a Fingerprint Sensor. *Sensors*, 17, 2280.

LexisNexis. (2016, May). *True Cost of Fraud Study.* Retrieved April 17, 2018, from https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf

LexisNexis. (2017, October). *True Cost of Fraud Study.* Retrieved November 1, 2018, from https://risk.lexisnexis.com/insights-resources/research/2017-true-cost-of-fraud-retail-study

LexisNexis Risk Solutions. (2015, January 26). *Press Release*. Retrieved from Fraud from Mobile Payments: http://www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1422223947870687

Lu, Y., Li, L., Peng, H., & Yang, Y. (2015). A biometrics and smart cards-based authentication scheme for multi-server environments. *Security and Communication Networks*, 8(17), 3219-3228. doi:10.1002/sec.1246

Matyas, V., Krhovjak, J., & Kumpost, M. (2008, February). Authorizing card payments with PINs. *IEEE Computer Society*, 64-68.

Mazzoni, M. 2013. Retrieved from Recycling PVC gift cards: http://www.earth911.com/living-well-being/recycling-mystery-gift-cards/

McDonald, Clare (2017). *Almost 70% of customers willing to use fingerprint biometrics to shop*. Retrieved 11 October, 2018 from Computer Weekly: https://www.computer weekly.com/news/450428775/Almost-70-of-customers-willing-to-use-fingerprint-biometrics-to-shop

Melodia, M., Bond, P., & Angelovska-Wilson, A. (2015). Legal Risks and Rules of the Move to Biometrics. *New York Law Journal*, 1-2.

Moganeshwaran, R., Mohamed, K., & Suhaini, M. *Fingerprint-Fingervein Multimodal Biometric Authentication System in Field Programmable Gate Array*. (IEEE, 2012), pp. 237-242.

Nasdaq. (2015, September 16). *Credit Card Fraud and ID Theft Statistics*. Retrieved from Nasdaq: http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388

Nichols, E. R. (2011). *Biotechnology in Agriculture, Industry, and Medicine.* New York, NY, USA: Nova.

Ozawa, N. (2015). *2015 Data Breach Fraud Impact Report.* San Francisco: Javelin Strategy & Research.

Pal, S. K., & Wang, P. P. (1996). *Genetic Algorithms for Pattern Recognition.* Boca Raton: CRC Press.

Papadimitriou, O. (2015, October 17). *Where Does Apple Pay Stand On Its First Birthday*. Retrieved from Tech Crunch: http://techcrunch.com/2015/10/17/where-does-apple-pay-stand-on-its-first-birthday/

Patterson, B. E. (2010). *Patent No. US8682798 B2.* United States.

Raj, S. E., & Portia, A. A. *Analysis on Credit Card Fraud Detection Methods*. (IEEE International Conference on Computer, Communication and Electrical Technology, March 2011), 152-156.

Randall, M. 2015. *Card Rates*. Retrieved from How Are Physical Credit Cards Made? http://www.cardrates.com/advice/how-are-physical-credit-cards-made/

B. Ruiz-Mezcua, D. Garcia-Plaza, C. Fernandez, P. Domingo-Garcia and F. Fernandez (1999). "Biometrics verification in a real environment," *Proceedings IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology (Cat. No.99CH36303)*, Madrid, 243-246.

Schaffer, T.M. 2015. *User acceptance of biometric smartcards for prevention of credit card fraud* (Doctoral dissertation).

Schmitt, J. C., & Setlak, D. R. (1997). *USA Patent No. US5903225 A.* Retrieved November 28, 2017, from https://www.google.com/patents/US5903225

Spraggs, D. (2007, February 1). *How to Lift Fingerprints*. Retrieved March 27, 2018, from http://www.policemag.com/channel/patrol/articles/2007/02/how-to-lift-fingerprints.aspx

Steele, J. (2017, October 24). *Credit card fraud and ID theft statistics* . Retrieved March 27, 2018, from https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php

K. L. Tang, A. Liu, W. Wang, P. Li, and X. Chen (2018). A novel fingerprint sensing technology based on electrostatic imaging. Sensors, 18, 1-10.

Tatham, M. (2018, March 15). *Identity Theft Statistics.* Retrieved November 12, 2018, from Experian: https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

Thomas, H., Jain, A., & Angus, M. 2013. The global journey from cash to cashless. *MasterCard Advisors' Cashless Journey*, 1-15.

United States Census Bureau. (2017, July 1). *Quick Facts United States.* Retrieved 17 November, 2018, from https://www.census.gov/quickfacts/fact/table/US/PST045217.

Weng. L-J., & Cheng, C-P. (2000). Effects of Response Order on Likert-Type Scales. *Educational and Psychological Measurement,* 60 (6). 908-924.

Williams, G. (2016, May 3). *Warning: ATM Fraud is on the Rise*. Retrieved March 30, 2018, from U.S. News: https://money.usnews.com/money/personal-finance/articles/2016-05-03/warning-atm-fraud-is-on-the-rise

Woodward, J. D. (1997). *Biometrics: Privacy's Foe or Privacy's Friend.* (IEEE, 1997), 1480-1492.

APPENDIX A: INSTRUMENT

________ Participant Number

Biometric Credit Card Survey

Please select your age category:

18-24	25-34	35-44	45-54	55+
□	□	□	□	□

Do you currently own a credit card?

YES	NO
□	□

Have you ever experienced credit card fraud against your credit card account?

YES	NO
□	□

With regards to biometrics as a means for authenticating a user in a credit card purchase, indicate ratings according to 1 thru 5 with 1 as "mostly disagree"; 2 as "disagree"; 3 as "neutral"; 4 as "agree"; and 5 as "mostly agree".

Statement: **Consumer Attitudes towards fraud**		**1**	**2**	**3**	**4**	**5**
Credit card fraud is a growing problem.	1.1					
Credit card companies currently have successful strategies to combat fraud.	1.2					
A company's ability to prevent fraud is important in the selection of a financial institution for obtaining a credit card.	1.3					
Credit card companies should utilize biometrics in order to protect customers from fraud.	1.4					
An occurrence of fraud leads to decreased trust in the financial institution.	1.5					
Successful prevention of a fraudulent transaction leads to increased trust in the financial institution.	1.6					
Statement: **Difficulty in using biometrics**						
Requiring biometric fingerprint data as part of a credit card application makes the application process too cumbersome.	1.7					
The use of biometric fingerprint for making a purchase transaction makes the transaction process easy and safe.	1.8					

With regards to biometrics as a means for authenticating a user in a credit card purchase, indicate ratings according to 1 thru 5 with 1 as "mostly disagree"; 2 as "disagree"; 3 as "neutral"; 4 as "agree"; and 5 as "mostly agree".

Statement: **Consumer attitude towards usage of biometrics for identity proofing.**		**1**	**2**	**3**	**4**	**5**
Providing a fingerprint as part of the credit card application increases financial account security.	2.1					
Utilizing the fingerprint at a point of sale terminal to validate a purchase transaction decreases the ability for a criminal to make a purchase on a stolen credit card.	2.2					
Utilizing the fingerprint on a mobile device to validate the account holder's identity decreases the ability for a criminal to make a purchase on a stolen mobile device.	2.3					
Use of my fingerprint to identify me as an account holder is more secure and decreases the chance for fraud to occur.	2.4					
Requiring fingerprint data will deter thieves from stealing physical credit cards.	2.5					

Indicate ratings according to 1 thru 5 with 1 as “mostly disagree”; 2 as “disagree”; 3 as “neutral”; 4 as “agree”; and 5 as “mostly agree”.

The use of biometric data for credit card fraud prevention will lead to increased instances of identity theft.	2.6					
The use of biometric data for credit card fraud prevention will decrease the ability for thieves to successfully utilize stolen identities.	2.7					
Statement: **Consumer attitude towards level of risk in using biometrics and acceptability.**		**1**	**2**	**3**	**4**	**5**
As a consumer, I feel comfortable providing my fingerprint at a point of sale terminal in order to validate that I am an account holder.	2.8					
As a consumer, I feel comfortable providing my fingerprint on a mobile device in order to validate that I am an account holder.	2.9					
I trust my financial institution with storing my fingerprint as part of my account information.	2.10					
I understand the risks involved in releasing my fingerprint data to a private institution.	2.11					
The risks involved in providing fingerprint data are less than the risks of credit card fraud.	2.12					

Indicate ratings according to 1 thru 5 with 1 as “mostly disagree”; 2 as “disagree”; 3 as “neutral”; 4 as “agree”; and 5 as “mostly agree”.

When using biometric data for user verification / account ownership validation, a backup process should be established to handle false declines.	2.13					
Statement: **Consumers’ attitude toward data privacy.**						
Requiring biometric fingerprint data is invasive and violates right to privacy.	2.14					

APPENDIX B: DATA MAPPING

Biometric Credit Card Survey - Question to Data Mapping

Demographics	
Age	Q1
Card ownership	Q2
Fraud experience	Q3
Fraud perceptions	1.1
Fraud perceptions	1.2
Fraud perceptions	1.3
Fraud perceptions	1.4
Fraud perceptions	1.5
Fraud perceptions	1.6
Ease of use	1.7
Ease of use	1.8
Attitude toward Identity Proofing	2.1
Attitude toward Identity Proofing	2.2
Attitude toward Identity Proofing	2.3
Attitude toward Identity Proofing	2.4
Attitude toward Identity Proofing	2.5
Attitude toward Identity Proofing	2.6
Attitude toward Identity Proofing	2.7
Attitude toward risk	2.8
Attitude toward risk	2.9
Attitude toward risk	2.10
Attitude toward risk	2.11
Attitude toward risk	2.12
Attitude toward risk	2.13
Attitude toward privacy	2.14

APPENDIX C: SAMPLE RAW DATA

Sample data includes the first 25 of 200 participant scores.

Age Category	Debit / Credit Owner	Fraud Victim
1.00	1.00	1.00
4.00	1.00	1.00
3.00	1.00	1.00
3.00	1.00	1.00
3.00	1.00	2.00
2.00	1.00	2.00
1.00	1.00	1.00
5.00	1.00	1.00
5.00	1.00	2.00
1.00	2.00	2.00
1.00	2.00	2.00
3.00	1.00	2.00
1.00	1.00	1.00
5.00	1.00	1.00
1.00	1.00	2.00
4.00	1.00	2.00
3.00	1.00	1.00
3.00	1.00	2.00
3.00	1.00	1.00
3.00	1.00	1.00
2.00	1.00	2.00
2.00	1.00	2.00
4.00	1.00	2.00
4.00	1.00	1.00
3.00	1.00	1.00

SAMPLE RAW DATA

CATEGORY: FRAUD PERCEPTIONS					
Fraud Growing Problem	Successful Strategies	Bank Selection	Use Biometrics	Fraud Trust	Prevention Trust
4.00	2.00	4.00	3.00	4.00	4.00
4.00	2.00	5.00	4.00	3.00	5.00
3.00	4.00	4.00	2.00	4.00	4.00
5.00	3.00	4.00	3.00	4.00	4.00
4.00	3.00	4.00	3.00	4.00	5.00
4.00	2.00	3.00	3.00	4.00	4.00
4.00	2.00	4.00	3.00	4.00	4.00
5.00	2.00	3.00	2.00	3.00	3.00
3.00	3.00	4.00	3.00	3.00	3.00
5.00	3.00	5.00	5.00	5.00	5.00
4.00	4.00	4.00	4.00	4.00	4.00
4.00	3.00	3.00	3.00	4.00	4.00
4.00	2.00	4.00	3.00	4.00	4.00
5.00	2.00	3.00	2.00	3.00	3.00
5.00	4.00	4.00	3.00	4.00	4.00
4.00	2.00	3.00	3.00	4.00	4.00
4.00	2.00	3.00	3.00	4.00	4.00
4.00	2.00	4.00	5.00	4.00	5.00

SAMPLE RAW DATA

CATEGORY: EASE OF USE		**CATEGORY: ATTITUDE TOWARD IDENTITY PROOFING**						
Biometric Cumbersome	Biometric Easy Safe	Financial Security	Biometric Decreases Fraud	Mobile	Biometric Identity	Biometric Deters	Biometric Increases Identity Theft	Biometrics Use Stolen Identities
3.00	4.00	4.00	4.00	4.00	4.00	4.00	2.00	4.00
2.00	4.00	4.00	4.00	4.00	4.00	4.00	2.00	4.00
4.00	4.00	4.00	5.00	5.00	4.00	3.00	3.00	4.00
2.00	4.00	3.00	2.00	4.00	4.00	1.00	3.00	4.00
3.00	4.00	3.00	5.00	4.00	5.00	4.00	2.00	4.00
2.00	4.00	4.00	4.00	4.00	4.00	4.00	3.00	4.00
4.00	4.00	3.00	4.00	4.00	4.00	4.00	2.00	4.00
4.00	1.00	2.00	2.00	1.00	1.00	1.00	4.00	3.00
1.00	4.00	3.00	4.00	4.00	4.00	4.00	1.00	4.00
2.00	5.00	5.00	5.00	5.00	5.00	5.00	3.00	3.00
3.00	4.00	4.00	4.00	4.00	4.00	4.00	3.00	3.00
4.00	4.00	4.00	4.00	4.00	3.00	3.00	3.00	3.00
3.00	4.00	4.00	4.00	4.00	4.00	4.00	2.00	4.00
4.00	1.00	2.00	2.00	1.00	1.00	1.00	4.00	3.00
4.00	4.00	2.00	4.00	4.00	4.00	3.00	2.00	4.00
2.00	4.00	4.00	4.00	4.00	4.00	4.00	2.00	4.00
2.00	4.00	3.00	2.00	4.00	4.00	1.00	3.00	4.00

SAMPLE RAW DATA

CATEGORY: ATTITUDE TOWARD RISK					
Consumer Comfort	Consumer Comfort Mobile	Institution Trust Bio Data	Biometric Risks	Bio Less Risk Fraud	Back Up Verification
4.00	4.00	3.00	2.00	3.00	4.00
4.00	4.00	2.00	4.00	4.00	5.00
4.00	4.00	1.00	5.00	1.00	4.00
3.00	3.00	1.00	5.00	2.00	4.00
2.00	3.00	1.00	4.00	3.00	5.00
4.00	4.00	3.00	3.00	3.00	3.00
4.00	4.00	3.00	2.00	3.00	4.00
3.00	1.00	1.00	3.00	2.00	3.00
4.00	4.00	4.00	4.00	4.00	4.00
5.00	5.00	3.00	2.00	3.00	5.00
4.00	4.00	3.00	2.00	2.00	4.00
3.00	4.00	3.00	2.00	2.00	4.00
4.00	4.00	3.00	2.00	3.00	4.00
3.00	1.00	1.00	3.00	2.00	3.00
4.00	3.00	3.00	2.00	4.00	4.00
4.00	4.00	2.00	4.00	4.00	5.00
3.00	3.00	1.00	5.00	2.00	4.00
3.00	3.00	1.00	5.00	2.00	4.00

SAMPLE RAW DATA

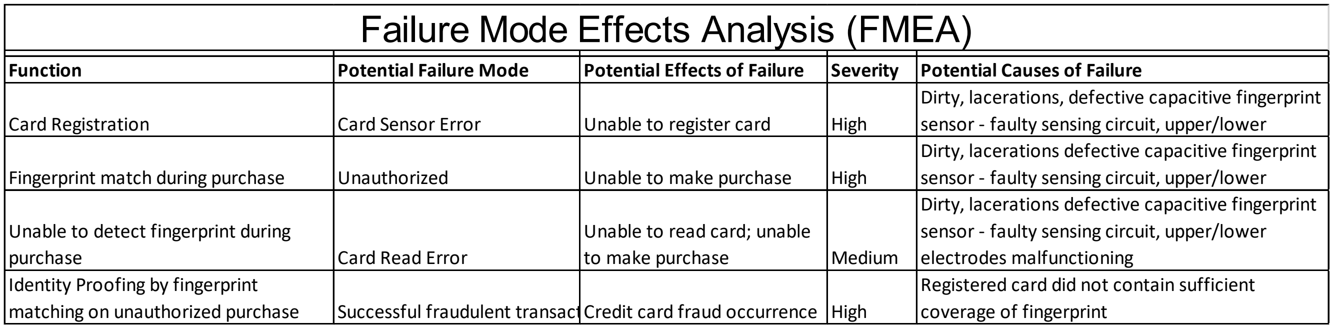
CATEGORY: ATTITUDE TOWARD RISK						CATEGORY: ATTITUDE TOWARD PRIVACY
Consumer Comfort	Consumer Comfort Mobile	Institution Trust Bio Data	Biometric Risks	Bio Less Risk Fraud	Back Up Verification	Biometric Invasive
4.00	4.00	3.00	2.00	3.00	4.00	2.00
4.00	4.00	2.00	4.00	4.00	5.00	2.00
4.00	4.00	1.00	5.00	1.00	4.00	3.00
3.00	3.00	1.00	5.00	2.00	4.00	4.00
2.00	3.00	1.00	4.00	3.00	5.00	2.00
4.00	4.00	3.00	3.00	3.00	3.00	2.00
4.00	4.00	3.00	2.00	3.00	4.00	2.00
3.00	1.00	1.00	3.00	2.00	3.00	4.00
4.00	4.00	4.00	4.00	4.00	4.00	2.00
5.00	5.00	3.00	2.00	3.00	5.00	3.00
4.00	4.00	3.00	2.00	2.00	4.00	3.00
3.00	4.00	3.00	2.00	2.00	4.00	3.00
4.00	4.00	3.00	2.00	3.00	4.00	2.00
3.00	1.00	1.00	3.00	2.00	3.00	4.00
4.00	3.00	3.00	2.00	4.00	4.00	2.00
4.00	4.00	2.00	4.00	4.00	5.00	2.00

SAMPLE RAW DATA

Biometric Card Raw Data Sheet for first 25 participants

Successful Registration Y/N	Successful Purchase 1st Attempt Y/N	Successful Purchase 2nd Attempt Y/N	Successful Fraud Attempt Y/N	Clean Dirty Print	Transaction Logs Biometric Data Present Y/N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	N	Y	N	D	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
N	N	N	N	C	N
Y	Y	N	N	C	N
Y	N	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	D	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	Y	N	N	C	N
Y	N	Y	N	C	N
Y	Y	N	N	C	N

APPENDIX D: FAILURE MODE EFFECTS ANALYSIS



Failure Mode Effects Analysis (FMEA)

Function	Potential Failure Mode	Potential Effects of Failure	Severity	Potential Causes of Failure
Card Registration	Card Sensor Error	Unable to register card	High	Dirty, lacerations, defective capacitive fingerprint sensor - faulty sensing circuit, upper/lower
Fingerprint match during purchase	Unauthorized	Unable to make purchase	High	Dirty, lacerations defective capacitive fingerprint sensor - faulty sensing circuit, upper/lower
Unable to detect fingerprint during purchase	Card Read Error	Unable to read card; unable to make purchase	Medium	Dirty, lacerations defective capacitive fingerprint sensor - faulty sensing circuit, upper/lower electrodes malfunctioning
Identity Proofing by fingerprint matching on unauthorized purchase	Successful fraudulent transact	Credit card fraud occurrence	High	Registered card did not contain sufficient coverage of fingerprint

APPENDIX E: INFORMED CONSENT

CONSENT TO PARTICIPATE IN RESEARCH

AN EVALUATION OF A BIOMETRIC ENABLED CREDIT CARD FOR PROVIDING HIGH AUTHENTICITY IDENTITY PROOFING DURING THE TRANSACTION AUTHORIZATION PROCESS

Your participation is requested in a research study conducted by Laura Poe and Xiaolong Li, from the Technology Management Program at Indiana State University. This study is being conducted as part of Laura Poe's dissertation to fulfill the requirements of the Doctor of Philosophy in Technology Management. **Your participation in this study is entirely voluntary.** Please read the information below and ask questions about anything you do not understand, before deciding whether or not to participate.

You have been asked to participate in this study in order to evaluate the capability of a biometric credit card's to perform higher levels of identity proofing and to determine if credit card fraud could be reduced by using biometric credit cards. Every year, credit cards are lost and stolen, and consumers experience fraud on their personal credit card accounts. The number of participants in this study will be 200, consisting of adults aged 18 and over, who are of legal age to obtain a credit card.

PURPOSE OF THE STUDY

The purpose of this study is to determine the reduction of the level of fraud related to lost/stolen/physical cards when utilizing biometric-enabled credit card devices, without requiring a financial institution to store the biometric data in order to protect both consumers and financial institutions, compared to the perceived reduction of fraud by consumers. The study will provide specific data related to the validity and feasibility of the biometric card, such as accuracy and error rates as well as fraud data comparisons. An evaluation of the data being passed in the background will determine the level of data privacy for the consumer.

PROCEDURES

If you volunteer to participate in this study, you will be asked to do the following things:

- Enroll your fingerprint in the biometric test credit card by placing the fingerprint on designated surface of the credit card and swiping the card across the merchant terminal. The fingerprint is read by the sensors and recorded directly into the card without transmitting any biometric data to the terminal or any other system.
- Make a mock purchase using the credit card terminal provided. The fingerprint will be placed on the credit card to validate the identity of the card holder by matching the registered fingerprint with the fingerprint on the card.
- Make a mock purchase using an alternate credit card. The fingerprint will be placed on the credit card to invalidate the identity of the card holder by denying access to the biometric credit card due to the mismatch of the registered card's fingerprint.
- Your fingerprint may be smudged using marker, dirt, fuzz, or a common substance to determine the interference of minutiae when attempting to make a transaction.
- Biometric credit cards will be destroyed following the purchase attempts.
- You will be asked to complete a brief survey to understand your perceptions of credit card fraud, biometric credit cards, and data privacy.
- Your participation is estimated to take approximately 15 minutes. The location of the procedures will take place at the research booth at the Short Pump Town Center in Glen Allen, VA.

POTENTIAL RISKS AND DISCOMFORTS

There are no associated risks or discomfort with this research There are minimal associated risks or discomfort with this research study. All biometric data is destroyed as part of the experimental procedures to eliminate the possibility of identity theft or data theft. Participation is completely voluntary and at the risk of the participant.

A subject may be withdrawn if unable to register any fingerprints.

POTENTIAL BENEFITS TO SUBJECTS AND/OR TO SOCIETY

Cost reduction for the merchants, credit card institutions, and average consumers as well as added security of financial data through the use of the biometric-enabled credit card could provide significant benefits to the financial industry by reducing fraud and identity theft risks for both consumers and credit card institutions. Additionally, the consumer could maintain the protection of their privacy using an integrated biometric fingerprint sensor that is built into the smartcard. This research seeks to determine if the combination of the existing chip card with the biometric credit card provides enhanced security and convenience for consumers and if the results support an expected reduction in credit card fraud.

CONFIDENTIALITY

No personal data is being stored as part of this research study. Participant's information will not be disclosed. Information will not be released to any other party for any reason outside of the purposes of this research study.

PARTICIPATION AND WITHDRAWAL

You can choose whether or not to be in this study. If you volunteer to be in this study, you may withdraw at any time without consequences of any kind or loss of benefits to which you are otherwise entitled. You may also refuse to answer any questions you do not want to answer. There is no penalty if you withdraw from the study and you will not lose any benefits to which you are otherwise entitled.

The investigator may withdraw you from this research if circumstances arise which warrant doing so. Such circumstances could be the inability to register the fingerprint on the test card or severe disruption by the participant to the study.

IDENTIFICATION OF INVESTIGATORS

If you have any questions or concerns about this research, please contact Laura Poe, Ph.D. Candidate; or Xiaolong Li, Faculty Sponsor.

Laura Poe
Lpoe2@sycamores.indstate.edu /
804-356-0918

Xiaolong Li
Xiaolong.li@indstate.edu
812-237-3457

RIGHTS OF RESEARCH SUBJECTS

If you have any questions about your rights as a research subject, you may contact the Indiana State University Institutional Review Board (IRB) by mail at Indiana State University, Office of Sponsored Programs, Terre Haute, IN 47809, by phone at (812) 237-3088, or e-mail the IRB at irb@indstate.edu. You will be given the opportunity to discuss any questions about your rights as a research subject with a member of the IRB. The IRB is an independent committee composed of members of the University community, as well as lay members of the community not connected with ISU. The IRB has reviewed and approved this study.

I understand the procedures described above. My questions have been answered to my satisfaction, and I agree to participate in this study. I have been given a copy of this form.

____

Printed Name of Subject

____ _________________________

Signature of Subject Date

IRBNet #: 1191429-3
Approved Date: August 21, 2018
Expiration Date: September 11, 2019
Indiana State University Institutional Review Board

APPENDIX F : STATISTICAL ANALYSES

Mean results of questions by category based on total participant pool of 200.

FRAUD PERCEPTIONS						EASE OF USE	
Fraud Growing Problem	Successful Strategies	Bank Selection	Use Biometrics	Fraud Trust	Prevention Trust	Biometric Cumbersome	Biometric Easy Safe
4.25	2.56	3.67	3.18	3.84	4.13	2.49	3.81

ATTITUDE TOWARD IDENTITY PROOFING						
Financial Security	Biometric Decreases Fraud	Mobile	Biometric Identity	Biometric Deters	Biometric Increases Identity Theft	Biometrics Use Stolen Identities
3.59	3.60	3.90	3.84	3.40	2.57	3.85

ATTITUDE TOWARD RISK						ATTITUDE TOWARD PRIVACY
Consumer Comfort	Consumer Comfort Mobile	Institution Trust Bio Data	Biometric Risks	Bio Less Risk Fraud	Back Up Verification	Biometric Invasive
3.71	3.59	2.27	3.35	2.93	3.97	2.63

STATISTICAL ANALYSES

Age Category

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	18-24	2	1.0	28.6	28.6
	25-34	1	0.5	14.3	42.9
	35-44	3	1.5	42.9	85.7
	45-54	1	0.5	14.3	100.0
	Total	7	3.5	100.0	
Missing	System	193	96.5		
Total		200	100.0		

Multivariate Tests[a]

Effect		*Value*	*F*	*Hypothesis df*	*Error df*	*Sig.*
Intercept	Pillai's Trace	1	8837.044[b]	2.000	189.000	0.000
	Wilk's Lambda	0.011	8837.044[b]	2.000	189.000	0.000
	Hotelling's Trace	93.514	8837.044[b]	2.000	189.000	0.000
	Roy's Largest Root	93.514	8837.044[b]	2.000	189.000	0.000
Age Category	Pillai's Trace	0.809	32.272	8.000	380.000	0.000
	Wilk's Lambda	0.305	38.324[b]	8.000	378.000	0.000
	Hotelling's Trace	1.906	44.794	8.000	376.000	0.000
	Roy's Largest Root	1.684	79.996[c]	4.000	190.000	0.000
Fraud Victim	Pillai's Trace	0.174	19.948[b]	2.000	189.000	0.000
	Wilk's Lambda	0.826	19.948[b]	2.000	189.000	0.000
	Hotelling's Trace	0.211	19.948[b]	2.000	189.000	0.000
	Roy's Largest Root	0.211	19.948[b]	2.000	189.000	0.000
Age Category * Fraud Victim	Pillai's Trace	0.485	15.210	8.000	380.000	0.000
	Wilk's Lambda	0.540	17.044[b]	8.000	378.000	0.000
	Hotelling's Trace	0.805	18.916	8.000	376.000	0.000
	Roy's Largest Root	0.742	32.252[c]	4.000	190.000	0.000

a. Design: Intercept + Age Category + Fraud Victim + Age Category * Fraud Victim

b. Exact statistic

c. The statistic is an upper bound on F that yields a lower bound on the significance level.

STATISTICAL ANALYSES

Recommend to Use Biometrics

Tukey HSD[a, b, c]

Age Category	N	1	2	3	4
55+	19	2.3158			
35-44	63		2.9841		
25-34	49		3.0000		
18-24	44			3.4091	
45-54	25				4.2400
Sig.		1.000	1.000	1.000	1.000

Means for groups in homogeneous subsets are displayed.

Based on observed means.

The error term is Mean Square (Error) = .198.

a. Uses Harmonic Mean Sample Size = 32.973

b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error
levels are not guaranteed.

c. Alpha = .05.

Tests of Between-Subjects Effects

Source	Dependent Variable	*Type III Sume of Squares*	*df*	*Mean Square*	*F*	*Sig.*
Corrected Model	Bank Selection	54.195[a]	9	6.022	40.343	0.000
	Recommend to Use Biometrics	67.338[b]	9	7.482	37.871	0.000
Intercept	Bank Selection	2033.990	1	2033.990	13626.891	0.000
	Recommend to Use Biometrics	1526.006	1	1526.006	7724.126	0.000
Age Category	Bank Selection	28.439	4	7.110	47.633	0.000
	Recommend to Use Biometrics	45.551	4	11.388	57.641	0.000
Fraud Victim	Bank Selection	0.390	1	0.390	2.611	0.108
	Recommend to Use Biometrics	6.272	1	6.272	31.746	0.000
Age Category * Fraud Victim	Bank Selection	15.295	4	3.824	25.618	0.000
	Recommend to Use Biometrics	15.333	4	3.833	19.403	0.000
Error	Bank Selection	28.360	190	0.149		
	Recommend to Use Biometrics	37.537	190	0.198		
Total	Bank Selection	2769.000	200			
	Recommend to Use Biometrics	2121.000	200			
Corrected Total	Bank Selection	82.555	199			
	Recommend to Use Biometrics	104.875	199			

a. R Squared = .656 (Adjusted R Squared = .640)

b. R Squared = .642 (Adjusted R Squared = .625)