

2016

An Empirical Investigation of Factors Affecting Resistance to Using Multi-Method Authentication Systems in Public-Access Environments

Joseph Marnell

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Databases and Information Systems Commons](#), and the [Information Security Commons](#)

Share Feedback About This Item

NSUWorks Citation

Joseph Marnell. 2016. *An Empirical Investigation of Factors Affecting Resistance to Using Multi-Method Authentication Systems in Public-Access Environments*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (970)
https://nsuworks.nova.edu/gscis_etd/970.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An Empirical Investigation of Factors Affecting Resistance to Using
Multi-Method Authentication Systems in Public-Access Environments

by

Joseph W. Marnell

A dissertation report paper submitted in fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2016

We hereby certify that this dissertation, submitted by Joseph Marnell, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Yair Levy, Ph.D.
Chairperson of Dissertation Committee

Date

Michelle Ramim, Ph.D.
Dissertation Committee Member

Date

Steve R. Terrell, Ph.D.
Dissertation Committee Member

Date

Approved:

Ronald J. Chenail, Ph.D.
Interim Dean, College of Engineering and Computing

Date

College of Engineering and Computing
Nova Southeastern University

2016

Abstract

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Empirical Investigation of Factors Affecting Resistance to Using
Multi-Authentication Systems in Public-Access Environments

by
Joseph W. Marnell
May, 2016

Over the course of history, different means of object and person identification as well as verification have evolved for user authentication. In recent years, a new concern has emerged regarding the accuracy of verifiable authentication and protection of personal identifying information (PII), because previous misuses have resulted in significant financial loss. Such losses have escalated more noticeably because of human identity-theft incidents due to breaches of PII within multiple public-access environments. Although the use of various biometric and radio frequency identification (RFID) technologies is expanding, resistance to using these technologies for user authentication remains an issue. This study addressed the effect of individuals' perceptions on their resistance to using multi-method authentication systems (RMS) in public-access environments and uncovered key constructs that may significantly contribute to such resistance.

This study was a predictive study to assess the contributions of individuals' perceptions of the importance of organizational protection of their PII, noted as Perceived Value of Organizational Protection of PII (PVOP), authentication complexity (AC), and invasion of privacy (IOP) on their resistance to using multi-method authentication systems (RMS) in public-access environments. Moreover, this study also investigated if there were any significant differences on the aforementioned constructs based on age, gender, prior experience with identity theft, and acquaintance experience with identity theft. As part of this study, a rollout project was implemented of multi-factor biometric and RFID technologies for system authentication prior to electronic-commerce (e-commerce) use in public-access environments. The experimental group experienced the multi-factor authentication and also was trained on its use. Computer users (faculty & students) from a small, private university participated in the study to determine their level of PVOP, IOP, and AC on their resistance to using the technology in public-access environments. Multiple Linear Regression (MLR) was used to formulate a model and test predictive power along with the significance of the contribution of the aforementioned constructs on RMS. The results show that all construct measures demonstrated very high reliability. The results also indicate that the experimental group of the multi-factor authentication had lower resistance than the control group that didn't use the technology. The mean increases indicate an overall statistically significant difference between the experimental and control groups overall. The results also demonstrate that students and participants' increased levels of education indicate an overall statistically significant decrease in resistance. The findings demonstrate that overall computer authentication training do provide added value in the context of measuring resistance to using newer multi-method authentication technology.

Acknowledgements

I would like to thank God, who gave me the strength to finish writing this dissertation. I am thankful for the support of my dissertation chair, Dr. Yair Levy, for his unending support, guidance, and always believing in me. I am thankful for my committee members, Dr. Michelle Ramim and Dr. Steven Terrell for their support, wisdom, as well as, guidance. To my two wonderful children, William and Paul, I want to thank you for your understanding and support of my education when I couldn't come and visit. I did this to leave you a trail to follow. I want to express my gratitude to my parents who are no longer with me, James Marnell and Shirley Marnell, who first showed their love for me by adopting me and my brother, Robert. I want to say thanks to my best friends, Jerry Perez, Larry Kuykendall, the McKinney family. I want to express my appreciation for the contribution and support that came from my university campus family, Dr. Bishop, and Dr. Unfred.

Table of Contents

Abstract ii

Acknowledgements iii

List of Tables ix

List of figures x

Chapters

1. Introduction 1

Background 1

Problem Statement 3

Dissertation Goal 7

Research Question and Hypotheses 10

Conceptual Model 12

Relevance and Significance 13

 Relevance 13

 Significance 14

Barriers and Issues 15

Limitations and Delimitations 15

 Limitations 15

 Delimitations 16

Definition of Terms 16

Summary 18

2. Review of Literature 20

Introduction 20

Perceived Value of Organizational Protection of Personal Identifying Information 21

Invasion of Privacy 24

Four Aspects of Privacy 25

Fair Information Practices 26

Authentication Complexity 28

Multi-Method Authentication Systems 30

Resistance to Using Multi-Method Authentication Systems 31

Contributions of this Study 33

3. Methodology 34

Research Design 34

Instrument Development 37

Validity and Reliability 40

Population and Sample 43

Pre-Analysis Data Screening 44

Data Analysis 46
Resource Requirements 49
Summary 50

4. Results 52

Overview 52
Exploratory Research (Phase I) 53
Delphi Method (Phase II) 53
Pre-Survey Selection and Training (Phase III) 54
Quantitative Research (Phase IV) 55
 Pre-Analysis Data Screening 55
 Descriptive Statistics Data Analysis 57
 Demographic Data Analysis 61
Summary of Results 74

5. Conclusions, Implications, Recommendations, and Summary 80

Overview 80
Conclusion 80
Implications 82
Limitations 83
Recommendations 84
Summary 86

Appendices 90

A. Survey Instrument for User of Multi-Method Authentication - Faculty- Multi-Method Authentication Systems 90
B. Survey Instrument for User of Multi-Method Authentication - Faculty- Username/Password Method 96
C. Survey Instrument for User of Multi-Method Authentication - Student-Multi-Method Authentication Systems 102
D. Survey Instrument for User of Multi-Method Authentication - Student- Username/Password Method 108
E. Expert Review Questionnaire 114
F. E-Mail to Expert Panel 116
G. Follow-up E-Mail to Expert Panel 118
H. E-Mail to Main Population 120
I. Follow-up E-Mail to Main Population 122
J. IRB Approval Letter to Collect Data from Wayland Baptist University 123
K. IRB Approval Letter to Collect Data from Nova Southeastern University 124

References 125

List of Tables

Tables

1. Summary Table of Authors and Constructs 36
2. Delphi Panel Experts 54
3. Delphi Panel Experts Recommended Adjustments to the Survey Instrument 54
4. Descriptive Statistics (Means and Standard Deviations) 57
5. Collinearity Statistics to Predict RMS 58
6. Matrix of Pearson Correlation of Coefficients 59
7. Cronbach Reliability Analysis 59
8. MLR Coefficients to Predict RMS 60
9. Adjusted R^2 and Standard Error to Predict RMS 60
10. ANOVA Interactions Results for PVOP, IOP, AC based on RMS 61
11. Descriptive Statistics of Age 61
12. Descriptive Statistics of Gender 62
13. Descriptive Statistics of Degree Major 62
14. Descriptive Statistics of Academic Level 63
15. Descriptive Statistics of Participants' Prior Experience with Identity Theft 63
16. Descriptive Statistics of Participants' Acquaintance Experience with Identity Theft 63
17. ANCOVA Results for PVOP, IOP, AC, and RMS based on Age 64
18. ANCOVA Results for PVOP, IOP, AC, and RMS based on Gender 65
19. ANCOVA Results for PVOP, IOP, AC, and RMS based on Degree Major 67
20. ANCOVA Results for PVOP, IOP, AC, and RMS based on Academic Level 68

21. ANCOVA Results for PVOP, IOP, AC, and RMS based on Participants' Prior Experience with Identity Theft 69
22. ANCOVA Results for PVOP, IOP, AC, and RMS based on Participants' Acquaintance Prior Experience with Identity Theft 71
23. T-Test Interaction Results for PVOP, IOP, AC, and RMS based on Student vs Faculty 72
24. T-Test Interaction Results for (Means and Standard Deviation) of PVOP, IOP, AC, and RMS based on Student vs Faculty 73
25. T-Test Interaction Results for PVOP, IOP, AC, and RMS based on MMAS or Not 73
26. T-Test Interaction Results for (Means and Standard Deviation) of PVOP, IOP, AC, and RMS based on MMAS or Not 74
27. A Summary of Research Question and Hypotheses and the Findings 77

List of Figures

Figures

1. Conceptual Model 12
2. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, on RMS based on Age 64
3. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Gender 65
4. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Degree Major 66
5. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Academic Level 68
6. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Participants' Prior Experience with Identity Theft 69
7. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Participants' Acquaintance Experience with Identity Theft 71

Chapter 1

Introduction

Background

Recent research suggested that electronic-commerce (e-commerce) transactions are not the primary source of identity theft (IDT) (Shareef & Kumar, 2012). However, Shareef et al. (2012) stated that IDT plays a substantial role in purchase resistance for consumers of e-commerce. Increasing demands to prevent IDT are advocated in recent literature, newspapers, and government policies. According to Shareef et al. (2012), “current research addresses the issues of identity theft; source, type, and preventative measuring tools” (p. 30). Additional studies indicated that inadequate user authentication (UA) methods are a contributing factor for IDT (Fichtman, 2001). A national survey conducted by the Federal Trade Commission (FTC) (2008) revealed that 4.7% of American adults experienced IDT that involved the loss of personal identifying information (PII). Industry responses to combat aspects of IDT are focused on the verifiable identification of individuals through the development of acceptable multi-method authentication systems (Bellah, 2001). While current research has reflected significant advances in biometric recognition, users continue to resist using biometric technology to enhance password security (Levy & Ramim, 2009). This resistance is attributed to concerns related to protecting their PII, invasion of privacy (IOP), and authentication complexity (AC).

The problem with IDT has escalated as a result of users sharing, reusing, and losing passwords, as well as the mishandling of PII during e-commerce transactions (Furnell, Dowland,

Illingworth, & Reynolds, 2000). This has resulted in significant losses from illegal authentication and theft of PII. Efforts to combat the weaknesses in current methods of username/password entries have influenced the development of biometric forms of identification (Altinkemer & Wang, 2011). However, single-authentication biometrics still exhibit misreads and errors, so organizations have turned to testing multi-method authentication systems for UA (Gunson, Marshall, Morton, & Jack, 2010). Increased monetary losses occurring due to privacy attacks during e-commerce activities within organizations have swayed individuals' perceptions of the importance of protecting PII (PVOP), lessened their use of Internet purchasing, and could influence their resistance to new authentication methods (Dowling & Staelin, 1995; Mayer, Davis, & Schoorman, 1995). Thus, this study was designed to empirically test the validity of a model on the contribution of the constructs of PVOP, IOP, and AC on individual's resistance to using multi-method authentication systems (RMS) in public-access environments. Additionally, this study addressed a gap in the UA literature linking UA and RMS. This was accomplished by assessing individuals' usage of RMS in a university setting.

The remainder of this investigation addressed individuals' RMS that undermines organizations' efforts to achieve enhanced protection of PII during UA, which was the guiding research problem for this study. Following the problem statement discussion is the main goal and the guiding research question. This study identified the hypotheses that stem from the main research question. Next, a discussion of this study's limitations, delimitations, and barriers is provided. Finally, this investigation concludes with a description of the approach that serves as the foundation for the methodology used by the study, while ending with definitions and a summary.

Problem Statement

The research problem investigated was identity-theft (IDT) incidents due to breaches of personal identifying information (PII) (Venkatesh, Morris, Davis, & Davis, 2003; Zviran & Erlich, 2006). Such PII breaches are significant threats to invasion of privacy (IOP) during e-commerce activities by users in public-access environments (Venkatesh et al., 2003; Zviran & Erlich, 2006). Kim, Jeong, Kim, and So (2011) identified PII as financial card numbers, usernames, passwords, medical records, driver's licenses, and Social Security numbers (Kim et al., 2011). These PII represent targets of online theft during e-commerce activities. Doolin, Dillon, Thompson, and Corner (2005) defined e-commerce as information networks that enable data flow for business, capital, and logistical support. Existing methods to protect PII during e-commerce activities are based on three types of authentication: username/password, tokens/smart cards, and biometrics (Levy & Ramim, 2009; Millett & Holden, 2003).

IDT is defined as the misuse of another individual's PII to commit acts of intentional fraud involving financial and personal information (Hinde, 2005; Wendels, Mählmann, & Versen, 2009). Financial-crime investigators regard IDT fraud as the intentional concealment of the illegal act of using another's identity to derive a benefit at someone else's expense (Bolton & Hand, 2002; Gottschalk, 2010). Jerman-Blažič and Klobucar (2005) defined IOP as "intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data" (p. 576). An IDT imposter commits these acts to obtain credit, merchandise, services, and money in the name of the victim (Laudon & Laudon, 2010).

It appears that individuals' perceptions of the importance of protecting PII, noted as Perceived Value of Organizational Protection of PII (PVOP), from financial and privacy attacks is related to their resistance to using various types of authentication (Dowling & Staelin, 1994;

Mayer et al., 1995). PVOP is defined as the value individuals place on protecting their PII, because of the potential consequences of being vulnerable to the actions of another party during e-commerce activities (Dowling & Staelin, 1994; Mayer et al., 1995). Prior research suggests that members of social media websites, for example, are experiencing increasing levels of PVOP because of IDT incidents from PII exposure (Nosko, Wood, & Molema, 2010).

Illegal access to PII enables an unauthorized person to use, copy, release, destroy, deny, or modify hardware, software, data, or network resources (O'Brien, 2002). According to Eisenstein (2008) and Kim et al. (2011), financial losses are incurred due to failure of merchants to protect customer data from unauthorized access. Such losses can occur as a result of stolen mail, computer data breaches, illegal access to Websites such as PayPal, computer viruses, phishing scams, packet sniffing, wiretapping, and paper-document theft (Eisenstein, 2008; Kim et al., 2011). Financial losses due to IDT incidents have deterred 75% of online users from attempting as many purchases (Lai, Li, & Hsieh, 2012).

Monetary losses incurred by individuals continue to increase as e-commerce payment activities flourish (Bhattacharyya, Jha, Tharakunnel, & Westland, 2011). A previous study of e-commerce purchases indicated that IDT occurrences can be influenced by demographics and geography (Higgins, Hughes, Ricketts, & Wolfe, 2008). These occurrences have resulted in 11.6 million victims in 2011, representing a 13% increase over 2010 (Javelin Strategy & Research, 2012). Publicly-reported security breaches for 2011 totaled 22,918,441 (Identity Theft Center, 2012).

The security breaches resulting from IDT incidents of PII have influenced efforts to reduce losses through improving authentication security (Altinkemer & Wang, 2011). According to Al-Harbi and Osborn (2011), user access involves users, roles, and authentication permissions that

allow specific interactions with a resource. The user interactions result in the flow of information based on specific privileges within permissible rules and error allowances (Al-Harbi & Osborn, 2011). According to Levy and Ramim (2009), authentication uses the two elements of identification and verification to validate an identity through “enabled authentication protocols that establish the identification processes between the host and the user” (p. 382).

User authentication (UA) methods that reduce PII loss include “something the user knows (e.g. password or personal identification number (PIN)), something the user has (e.g. a card or other token) and something the user is (e.g. a biometric characteristic)” (Furnell, Papadopoulos, & Dowland, 2004, p. 529). Complexities of multiple layers of UA appear to be increasing (Barton, Byciuk, Harris, Schumack, & Webster, 2005). Furthermore, various biometrics are interpreted incorrectly and issue high false-rejection rates (FRR). These multiple layers represent combinations of unique biometric physical or behavioral characteristics currently used for validating authentication with hand, eye, face, or voice features (Barton et al., 2005).

Millett and Holden (2003) defined UA as any identifier-forming process that distinguishes an individual's username/password, token/smart card, retina, voice, or other forms of recognition. Furnell et al. (2000) stated that UA is “an essential first line of defense in the security of Information Technology systems” (p. 529). According to Chandra and Calderon (2005), accurate identification, as well as verification, of users is based on confidentiality, availability, integrity, authorization, audit, and non-repudiation factors. While users prefer the simplicity of traditional username/password authentication, history reflects those methods are limited and not a strong enough means of authentication (Adams & Sasse, 1999). These limitations are attributed to password attacks by malware, phishing, and reuse technologies (Adams & Sasse, 1999).

Furnell et al. (2000) defined authentication complexity (AC) as issues that complicate UA based on effectiveness, cost, and user acceptance. Other issues adding complexity to UA include users' tokens being lost, stolen, or misplaced, as well as sharing, forgetting, and reusing passwords (Furnell et al., 2000). The increase of malicious attacks on systems to obtain PII is intensifying AC (Pearce, Zeadally, & Hunt, 2010). Gritzalis (2004) suggested that protection from IOP was based on users' "ability to control the terms by which their personal information is collected and used" (p. 195). However, users willingly choose to overlook IOP to minimize AC by circumventing security methods in favor of expediency and practicality (Adams & Sasse, 1999). Thus, a simpler, more secure UA that minimizes AC may need to be established by utilizing multiple means of authentication that are verifiable, effective, affordable, and user-friendly (Furnell et al., 2004; Tsalakanidou, Malassiotis, & Strintzis, 2007). Conversely, enhancing security may result in increasing the complexity of authentication methods (Furnell et al., 2004; Tsalakanidou et al., 2007).

Resistance to using multi-method authentication systems (RMS) is defined as the reluctance to accept alternative methods of user verification due to perceived security, complexity, and privacy concerns (Bellah, 2001; Van Hoose, 2008). Such resistance has been linked to various types of authentication systems (Jones, 1991; Wang & Petrison, 1993). Resistance can also be attributed to intrusiveness and the perception of potential IOP (Zviran & Erlich, 2006). Industry trends are moving toward the use of multi-method authentication systems with recognizable biological human characteristics beyond the traditional fingerprints that include DNA, voice recognition, and eye patterns (Bolton & Hand, 2002; Gottschalk, 2010). In fact, 83% of mobile users indicated an acceptance of some form of biometrics for improved mobile telephone security, while more than 30% were unwilling to use currently available pin-type methods

because of problems related to AC (Clarke & Furnell, 2005). Some research suggests that expectation of improved authentication accuracy with less complexity could decrease RMS (Clark & Furnell, 2005; Jain & Ross, 2004; Levy & Ramim, 2009; Ross, Nandakumar, & Jain, 2006). However, because of the increasing complexity of previous UA methods, the use of defense-in-depth approaches with multi-method authentication systems is escalating (Pearce et al., 2010).

According to Jones (1991), as well as Wang and Petrison (1993), it appears that individuals' perceptions of the importance of protecting their PII is related to their resistance to using various types of multi-method authentication systems. Having said that, little is known about the role of individuals' perceptions of authentication complexity and the importance of protecting their PII on their RMS. Therefore, it appears that additional research on the factors of authentication complexity, perceived invasion of privacy, and individuals' perceptions about the perceived value of organizational protection of their PII is warranted in predicting resistance to using various types of authentication.

Dissertation Goal

The main goal of this proposed research study was to assess empirically individuals' perspectives on the contribution of perceived value of organizational protection of their personal identifying information (PII) (PVOP), perceived invasion of privacy (IOP), and authentication complexity (AC) on their resistance to using multi-method authentication systems (RMS) in public-access environments. PVOP, IOP, and AC are the independent variables (IV) in this research study. The dependent variable (DV) in this research study is RMS. This research study assessed the difference in PVOP, IOP, AC, and RMS in public-access environments based on

individuals' age (AGE), gender (GEN), degree major (DM), academic level (AL), prior experience with identity theft (EXP), and acquaintance experience with identity theft (EXA), the six control variables. Assessing RMS during e-commerce activities may reveal how best to lower IDT losses (Doolin et al., 2005; Roussos & Moussouri, 2004). This study builds on previous research by Altinkemer and Wang (2011), as well as Roussos and Moussouri (2004), which suggested that the integration of multi-method authentication systems for identity verification in public-access environments could minimize IDT. Furthermore, Altinkemer and Wang (2011) recommended additional research into multi-method authentication systems to secure user authentication entries. Prior research by Klaus, Wingreen, and Blanton (2010) suggested that reducing losses from goods and services purchased illegally through IDT will require institutions to provide a means of minimizing the number of users affected by AC.

According to Venkatesh et al. (2003), resistance to accepting emerging technology is based on the difference between an individual's non-adoption and his or her acceptance levels. Thus, resistance on the part of individuals may be the cause of significant failures in the implementation of multi-method authentication systems (Robey, Ross, & Boudreau, 2002). Furthermore, previous studies in ubiquitous environments suggested that numerous factors can influence individuals' resistance to technology (Karyda, Gritzalis, Park, & Kokolakis, 2009). Although PVOP, IOP, and AC have all been referenced in prior research, it appears that very little attention has been given to the development of a predictive model of RMS that incorporates such constructs in public-access environments. Therefore, despite the many benefits of multi-method authentication systems noted by researchers (Attaran, 2006; Gunson et al., 2010; Levy & Ramim, 2009; Roussos & Moussouri, 2004), a considerable number of individuals are still not using multi-method authentication systems to conduct e-commerce activities. Moreover, a

significant number of individuals consider the authentication process to be too complex or too invasive of their protected information (Attaran, 2006; Gunson et al., 2010; Levy & Ramim, 2009; Roussos & Moussouri, 2004). However, this has not deterred substantial numbers of retailers and government agencies from testing various forms of biometrics for identification purposes (Clodfelter, 2010). Biometric systems use two phases of operation consisting of enrollment and authentication. The enrollment process requires the collection of biometric data, identity linking, and storage through the various forms of biometric technology such as fingerprint scanning. The authentication process consists of the verification of an individual against the enrollment biometric data collected previously (Clodfelter, 2010).

Previous studies suggested that divergent age levels exhibiting different responses and intentions could be useful for identifying potential IDT expectations (Venkatesh et al., 2003; Zviran & Erlich, 2006). To help address and reduce IDT, the IVs warrant further research, since much of the prior research regarding factors affecting RMS focused on IVs separately (Venkatesh et al., 2003; Zviran & Erlich, 2006). Despite the previous literature, little attention has been given to assessing PVOP, IOP, and AC as they relate to individuals' age (AGE), gender (GEN), degree major (DM), academic level (AL), prior experience with identity theft (EXP), and acquaintance experience with identity theft (EXA), demographic indicators which appear to affect resistance to using RMS in public-access environments.

This study builds on previous work with types of human, object, and biometric authentication methods by Attaran (2006), Gunson et al. (2010), Levy and Ramim (2009), as well as Roussos and Moussouri (2004) that might warrant consideration as a way to reduce RMS within the context of public-access environments. There are six specific goals of this research study. The first three specific goals are to investigate empirically the contribution of PVOP, IOP, and AC to

RMS, respectively, in public-access environments. The fourth specific goal is to investigate empirically the contribution of the interaction of the three independent variables, PVOP, IOP, and AC on individuals' RMS in public-access environments. The fifth specific goal is to investigate empirically whether any significant differences of PVOP, IOP, AC, and RMS exist based on individuals' age (AGE), gender (GEN), degree major (DM), academic level (AL), person's prior experience with identity theft (EXP), and person's acquaintance experience with identity theft (EXA). The sixth specific goal is to investigate empirically whether any significant differences of PVOP, IOP, AC, and RMS exist based on individuals who have used the multi-method authentication system and those who haven't, as well as, student and faculty, in public access environments.

Research Question and Hypotheses

The main research question (RQ) that this study addressed was: What is the contribution of PVOP, IOP, AC, and the interaction on individuals' resistance to using multi-method authentication systems in public-access environments?

In addressing the main RQ, this study addressed 11 specific hypotheses (noted in null form):

H1: *Individuals' Perceived Value of Organizational Protecting PII (PVOP)* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H2: *Invasion of Privacy (IOP)* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H3: *Authentication Complexity (AC)* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H4: There will be no significant interaction effect of *PVOP*, *IOP*, and *AC* on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H5a: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on age (*AGE*).

H5b: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on gender (*GEN*).

H5c: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's degree major (*DM*).

H5d: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on academic level (*AL*).

H5e: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's prior experience with identity theft (*EXP*).

H5f: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's acquaintance experience with identity theft (*EXA*).

H6: There will be no statistically significant differences on *PVOP*, *IOP*, *AC*, and *RMS* based on individuals who used a multi-method authentication system in public-access environments and those who haven't, as well as Student and Faculty in public-access environments.

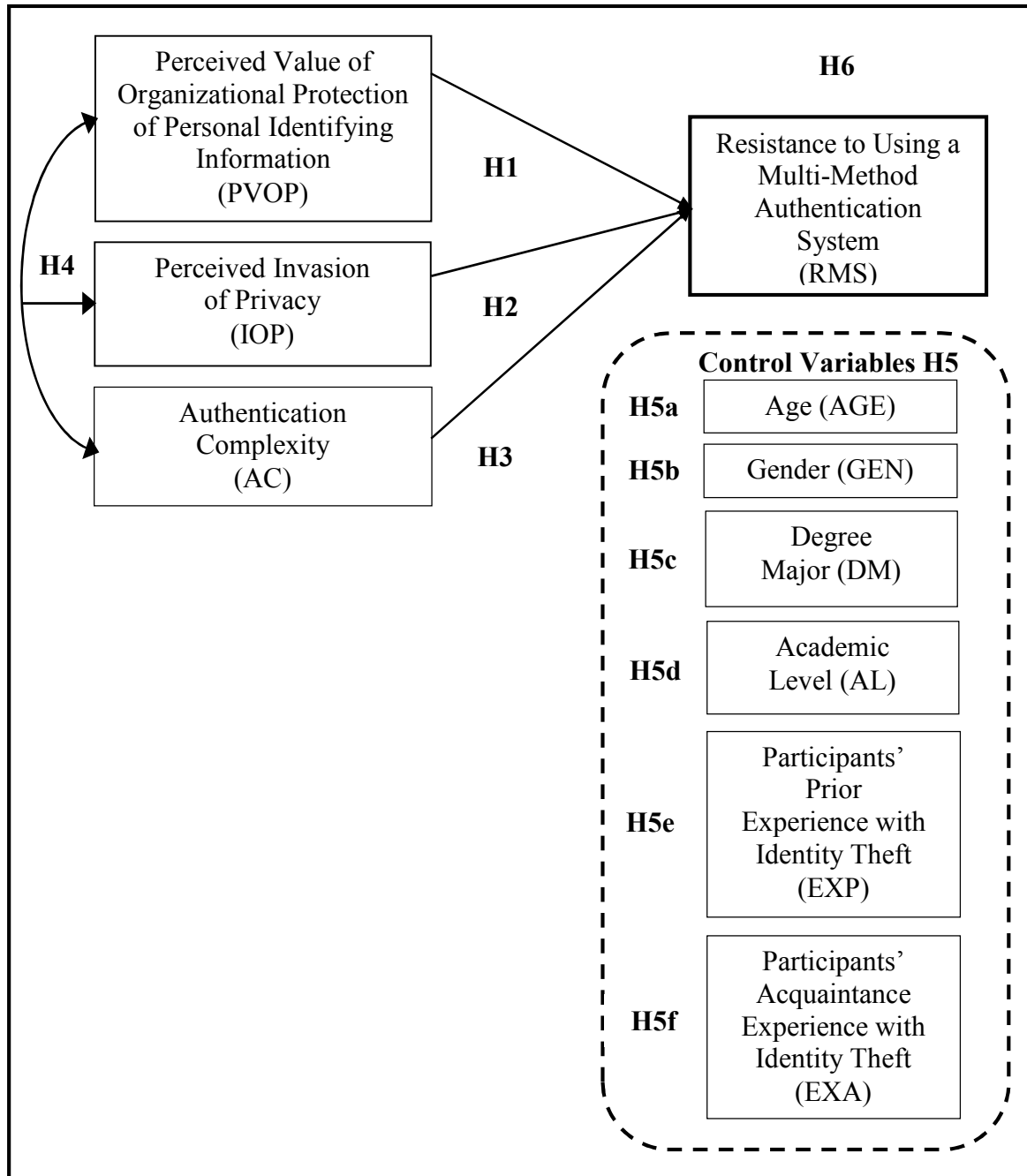


Figure 1. Conceptual Model for Predicting RMS in public-access environments.

Relevance and Significance

Relevance

This study provided further research into the factors that influence individuals' RMS (Gunson et al., 2010). However, a review of the literature reveals limited studies focusing on resistance to using multi-method authentication systems as it relates to minimizing IDT in public access environments. This study is relevant, as it investigated users' RMS in public-access environments, leading to an improved understanding of the factors that contribute to user multi-method authentication resistance. The public access areas encompass sporting events, national and state borders, hospitals, as well as airports. According to Anderson et al. (2008), in a survey conducted by the Federal Trade Commission (FTC) (2003), IDT was considered one of the greatest threats to the U.S. economy. Additional surveys were conducted by Gartner, Inc. in 2003, as well as the American Association of Retired Persons (AARP) and the U.S. Department of Justice Bureau of Justice Statistics in 2006 (Anderson et al., 2008). Furnell (2007c) indicated that false identity, identity theft in the form of PII, and other forms of impersonation now affecting an increasing number of victims are due to the attractiveness of these financial propositions to criminals. Thus, identity fraud leading to theft can be accomplished easily by only gaining someone's name and address to cause them significant inconvenience through impersonation (Furnell, 2007a). Furthermore, Furnell and Clarke (2012) implied that in spite of technological advances and the strengthening of policies, people represent a critical element for the achieving or failing of security systems that protect PII. Equally important was the study by Allison, Schuck, and Lersch (2005), which indicated that the reporting of "identity theft appeared to be larger than those of other theft-oriented offenses-credit card fraud, check fraud, robbery, and motor vehicle theft" (p. 28). While IDT is not as interesting as crimes of violence, it does

require more research to alleviate its impact on society (Allison et al. (2005). An additional research study examined username/password-authentication methods related to biometric mechanisms (Venkatesh et al., 2003). However, the consensus among researchers is that more focus needs to be placed on AC, as it significantly impacts PII security (Furnell, 2007b; Levy, 2007c). According to Furnell (2008), increasing use of PII by merchants and e-commerce users' misuse of passwords, places individuals at greater risk of IDT, as well as requires greater protection of remotely stored PII.

Significance

This research is significant, as it advanced current research in resistance to using various forms of multi-method authentication systems by increasing the body of knowledge regarding the factors that contribute to individuals' authentication behaviors in public-access environments. The impact of illegal access to PII from the ongoing practice of carelessly sharing and reusing passwords increases financial risks to users (Hazari, Hargave, & Clenney, 2008; Furnell, 2008). The potential results of the study provided valuable information that could influence future strategies to secure user authentication identification, as well as address the need for further examination of individual RMS (Doolin et al., 2005; Palmer, 2008). This could potentially help to lower IDT occurrences by examining multi-method authentication systems that influence users' resistance to technology.

Insight into strategies for reducing the complexity of multi-method authentication systems through biometrics is of significance to all who participate in e-commerce (Nandakumar, 2008). According to Hazari et al. (2008), understanding users' password behaviors could be of significance when examining AC. Enhanced forms of cyber security risks are becoming more prevalent, especially those involved in the fight against increasing IDT (Identity Theft Resource

Center, 2012). User authentication is considered a privacy risk for government, corporations, and users of e-commerce (Doolin et al., 2005). Achieving a secure means of user authorization for e-commerce transactions would greatly assist hospitals, businesses, and government organizations in developing, as well as implementing strategies, programs to secure PII effectively, while preventing IDT (Doolin et al., 2005; Palmer, 2010).

Barriers and Issues

There were a number of potential barriers to this study. One such barrier was obtaining the permission required to survey students and instructors as survey participants. Additionally, Institutional Review Board (IRB) approvals from two universities were required to conduct this study.

Limitations and Delimitations

Limitations

One limitation of this study was measuring the RMS of participants who were asked to respond to hypothetical scenarios, and who may not have understood all that was required to answer the questions. Compeau and Higgins (1995) recommended that individuals be asked to provide responses to the experiences they encounter by imagining future uses of various technologies. Thus, the level of difficulty in identifying individuals' RMS was measured through a participant survey that required the use of biometric and/or RFID for user authentication in e-commerce in public-access environments. According to Bandura (1977), survey participants should be required to answer questions based on fixed patterns of responses. In addressing this issue during the quantitative phase of this study, an expert review panel evaluated the quantity

and clarity of the questions, as well as the precision of the measurement instrument. Thus, an expert panel was created using both quantitative and qualitative methods to examine the survey instrument's validity, while recommending modifications where needed.

Two further limitations were the self-reporting of prior password conduct that influences personal behaviors, trust, and attitudes reflected in PVOP, IOP, AC, and RMS. According to Verplanken and Orbell (2003), acknowledgment of prior behaviors and experiences of users' passwords, as well as privacy concerns is not easily obtained. Additionally, there were equipment requirements to conduct the study that were not publicly available.

Delimitations

This study was delimited to students and staff from a single, private university located in the southwestern U.S. This study was limited to biometric scanning of fingerprints and RFID scanning with USB plug-in adapters, as well as a traditional username/password single sign-on authentication with a Windows 7 operating system. This method of authentication allowed user profiles that were capable of being identified remotely through an enterprise-wide area network that authenticates through a Windows server 2012 active directory system.

Definition of Terms

The following outlines various terms, as well as acronyms used along with their definition and description:

Access – Users, roles, and authentication permissions that allow specific interaction with a resource that influences the flow of information based on specific rights, as well as privileges within permissible rules and error allowances (Al-Harbi & Osborn, 2011).

Authentication – Any process of forming identifiers that distinguish individual usernames and passwords along with smart cards, retina scans, voice, or other forms of recognition (Millett & Holden, 2003).

Authentication Complexity (AC) – The degree to which an innovation is perceived as relatively difficult to understand, use for access, and authentication for electronic-data transfer in public-access environments (Uzoka & Ndzingo, 2009).

Electronic-Commerce (e-commerce) – Computer electronic online commerce through information networks that enable data flow for business, capital, and logistical support (Doolin et al., 2005).

Identity Theft (IDT) – An imposter’s intentional theft of PII to obtain credit, merchandise, or services in the name of the victim (Eisenstein, 2008; Kim et al., 2011).

Identity Theft Experiences (EXP) – Incidents in which individuals are actually affected by the intentional theft of PII by an imposter to obtain credit, merchandise, or services in the name of the victim (Kim et al., 2011).

Invasion of Privacy (IOP) – Intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual (Jerman-Blažič & Klobucar, 2005).

Perceived Value of Organizational Protection of Personal Identifying Information (PVOP) – The value an individual places on the potential loss of his or her personal identifying information, represented by his or her driver’s license, credit card, Social Security number, and personal health information that places him or her at a great risk if not protected by organizations (Doolin et al., 2005).

Personal Identifying Information (PII) – Credit and debit card numbers, usernames, passwords, medical records, driver’s license, and Social Security number representing an individually unique person (Kim et al., 2011).

Resistance to Using Multi-Method Authentication Systems (RMS) – A measure of someone’s aversion to using a certain type of authentication, based upon type and sensitivity (Jones, 1991; Wang & Petrison, 1993).

Summary

The purpose of chapter one is to introduce the study, identify the research problem, discuss, and recognize any barriers, as well as limitations to conducting this study, and to provide a theoretical basis for this study. The research problem this study addressed is identity-theft (IDT) incidents due to breaches of personal identifying information (PII) are significant threats to invasion of privacy (IOP) during e-commerce activities by users in public-access environments. Valid literature supporting the need for this research was also presented. Moreover, chapter one also presented the main goal, specific goals, and specific research questions that were addressed through this study. The main goal of this study addressed empirically individuals’ perspectives on the contribution of perceived value of organizational protection of their personal identifying information (PVOP), perceived invasion of privacy (IOP), and authentication complexity (AC) on their resistance to using multi-method authentication systems (RMS) in public-access environments. Prior literature that supports the main goal of this research was presented (Altinkemer & Wang, 2011; Attaran, 2006; Doolin et al., 2005; Gunson et al., 2010; Karyda, Gritzalis, Park & Kokolakis, 2009; Klaus, Wingreen, & Blanton, 2010; Levy & Ramim, 2009;

Gunson et al., 2010; Robey, Ross, & Boudreau, 2002; Roussos & Moussouri, 2004; Venkatesh et al., 2003).

Chapter 2

Review of the Literature

Introduction

A search for previous models of implementation success validated that similar constructs related to user satisfaction, system quality, information quality, and IS service quality consistently appeared in prior studies (DeLone & McLean, 1992, 2003). While these identified constructs are valid, the purpose of this study moved beyond previously recognized and validated constructs by examining other individual constructs that appear promising as predictors of multi-method authentication systems resistance. More specifically, the implementation success from the perspective of reduced resistance as described within this investigation focused only on the constructs of PVOP, IOP, AC, and RMS. Therefore, a brief review of the literature for each of these key constructs was provided as a theoretical foundation for this study. This section includes the results of a literature search in a variety of areas that included multi-method authentication systems technology, IS security, identity theft, perceived value of organizational protection of personal identifying information, invasion of privacy, behavior, user resistance, intention to use technology, sociology and psychology, biometrics, radio frequency identification (RFID), authentication complexity, e-commerce, password usage, and research methodology.

This review presented the literature on the constructs of identity theft, e-commerce, and users' resistance to using multi-method authentication systems technology, privacy concerns, authentication complexity, password issues, and user behavior, in the context of the larger

construct of resistance to using new methods of authenticating in public access environments. The literature review began with a search on perceived value of organizational protection of personal identifying information and invasion of privacy, and ended with authentication complexity, as these are the three independent variables of this study. Finally, the literature review focused on resistance to using multi-method authentication systems in light of user password threats leading to significantly larger losses to individuals, as this is the dependent variable in this study.

Perceived Value of Organizational Protection of Personal Identifying Information

According to Dowling and Staelin (1994), as well as Mayer et al. (1995), the PVOP of PII is demonstrated by the elevated concerns of IOP resulting from financial losses occurring from IDT. These losses are increasing due to individuals exhibiting unsafe password behaviors such as reusing and sharing passwords, as well as the lack of awareness of the costs associated with PII theft (Eisenstein, 2008; Furnell, 2008; Kumar, Mohan, & Holowczak, 2008; Levy, 2008). Users are unaware that illegal access to PII enables unauthorized access to use, copy, and release, destroy, deny, or gain access to create imposter accounts (Furnell, 2008; Obrien, 2002; Rezgui & Marks, 2008; Shaw et al., 2008).

According to Eisenstein (2008), PII loss stems from a variety of causes, resulting in significant financial loss. These occurrences include merchant failures to protect client data under their personal control, stolen mail, computer data breaches, as well as illegally reproduced pay sites such as PayPal, viruses, and phishing scams (Furnell, 2008; Kumar, 2008; Shaw et al., 2008). Furnell (2008) identified users as (a) those informed of areas of IDT risk who are doing something to protect themselves, as opposed to (b) those who remain indifferent to the

seriousness of the loss of PII. This study followed the examples of Eisenstein (2008), Furnell (2008), Nosko et al. (2010), as well as Shareef and Kumar (2012), who considered individuals who took inadequate measures to protect themselves by being inadequately informed as being at greater risk of IDT due to the loss of personal identifying information that stems from an IOP.

According to Kim et al. (2011), the need to protect PII is reflected in the vast landscape of opportunities for theft. Financial card numbers, usernames, passwords, medical records, drivers' licenses, and Social Security numbers are defined as PII. These are some of the primary targets for online theft. The definition of PII is supported in literature through a review of user awareness of their PII and the need to protect it (Furnell, 2008; Kim et al., 2011; McDaniel, 1994).

In a group of three studies of 400 randomly selected, accessible, personal profiles from eight Canadian FacebookTM networks, Nosko et al. (2010) investigated the following: (a) a checklist instrument to summarize disclosed PII on FacebookTM profiles, (b) PII at most risk of disclosure in banks, schools, and jobs in potentially threatening ways, and (c) which, age, gender, relationship, and network had the most influence on which user was most likely to reveal PII. For some of the online social networking participants, a significant quantity of PII was shared, and certain types of data were determined to be more likely to be revealed than other data types. However, those items containing personal contact information did not result in substantial conclusions due to factors such as age, gender, marital relationship status or a connection to a particular network. However, one significant trend reflected that, as age increased, so did trust issues regarding PII loss security concerns. Therefore, age became an easy target of value by illegal users due to the extremely sensitive nature of PII. According to Nosko et al. (2010), their "study was important because it provided evidence that highly personal, sensitive, and

potentially stigmatizing information is being disclosed on social networking sites” (p. 416).

Therefore, some users express greater caution regarding PII exposure due to the increasing evidence of online identity theft and cyber bullying occurrences. Thus, the results of their study indicate the need for further development of programs and interventions to protect users, as well as their PII that may be at risk through identity exposure (Nosko et al., 2010).

In a second study, Furnell et al. (2008) investigated 20 novice users’ (a) understanding of the potential security threats to their PII, (b) awareness, as well as usage, of security measures required to protect PII, (c) perceptions and behaviors regarding PII security measures, and (d) other related factors that restrict protection of the users’ PII online. Furthermore, recent evidence indicates home users are now targets in 95% of attacks (Symantec, 2006). According to Furnell et al. (2008) evidence suggests that users are “ultimately responsible for their own systems, and may often lack the knowledge or inclination to take steps to protect themselves” (p. 235). Furthermore, sample results indicated that novice users have credibility issues with online behavior which include password, credit, and debit card usage, anti-virus programs, as well as safe site viewing. Furnell et al. (2008) suggested that users indicated a “lack of understanding of both the potential impact of the threats and the required scope of protection” (p. 237). However, the interview transcripts indicate that novice users had some exposure to threats that placed their PII at risk, with credit card, online banking, and malware being the most recognizable categories identified. Thus, novice users’ exhibited a level of interest in learning methods that might better protect their PII (Furnell et al., 2008).

Invasion of Privacy

According to Altman (1976), the “concept of privacy appears in the literature of several disciplines-psychology, sociology, anthropology, political science, law, architecture, and the design professions” (p. 7). Furthermore, privacy is considered an interpersonal boundary control process that accentuates seclusion, withdrawal, and the avoidance of interaction with others. According to Westin (1967), the part of the individual in this epic battle of PII disclosure indicates that:

Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives (p. 7).

According to Bonner and Chiasson (2005), in spite of the extensive investigations of “privacy in research, government legislation and commercial privacy policies, concerns about privacy continue to increase” (p. 269). Thus, a careful analysis of historical privacy legislation suggests that the Fair Information Practices that girds up such legislation leads towards reducing rather than protecting privacy. However, Furnell and Clarke (2012) stated that the varying security elements that require active participation by end users in any environment necessitating authentication places those users at risk for IOP are comprised of behaviors, designs, deployments, configurations, and maintenance of systems.

Current IT security efforts are attempting to minimize the incidents leading to IOP. According to Furnell and Thomson (2009), human aspects of password misuse due to AC, securing of PII, and understanding individuals’ behaviors towards protecting their PII are considered major challenges. According to Johnston, Eloff, and Labuschagne (2003), users

demonstrate a need to better acquaint themselves with the impact that security breaches encompass. Consequently, factors such as trust and certainty related to user interfaces, as well as performance reliability are impacting users' attitudes, perceptions, and behaviors that have led to increased resistance to using multi-method authentication systems (Furnell & Clarke, 2012). However, the increased awareness of the importance of securing user PII is now motivating users towards multi-method authentication (Danchev, 2011). The result has been a recently-instituted group within the Institute of Fair Information Practices (IFIP) named WG11.12 on Human Aspects of Information Security and Assurance (see www.ifip11-12.org) dedicated to these factors. The overall scope of this research is the modifying of human behaviors or multi-method authentication systems to reduce complexities and IOP (Furnell & Clarke, 2012).

According to Hough (2009), privacy crusader Alan Westin defined privacy as “the claim of individuals, groups, or institutions to determine for themselves, when, where, how, and to what extent information about themselves is communicated to others” (p. 7). However, Westin's contemporary, David Flaherty, separated privacy further into four aspects of privacy sections.

Four Aspects of Privacy

Solitude: the perfect and unblemished state of privacy whereby you can easily restrict access to yourself from others by withdrawing your presence.

Intimacy: this is by membership only and groups protect their members.

Anonymity: this is a form of being “off the grid” in that you are able to protect yourself from ongoing public recognition or involvement.

Reserve: this is the measure of trust that one places in others not to disclose specific information about oneself, such as what, where, when, and how (Hough, 2009).

According to Karyda and Gritzalis (2009), privacy can generally be defined as “the individual’s ability to control the terms by which their [sic] personal information is collected and used” (p. 195). Thus, the prevention of IOP could represent protection or freedom from interference by others (Gritzalis, 2004). The concept of acknowledging an individual’s right to privacy includes the factors of necessity, finality, transparency, and proportionality (Karyda & Gritzalis, 2009).

Karyda and Gritzalis (2009) stated that *necessity* refers to the need for using PII, as well as recognizing other means of user identification, such as multi-method authentication systems. *Finality* identifies the usage of PII for legitimate purposes. *Transparency* recognizes individuals’ responsibility to be aware of how their PII is collected, whether by means of notification or consent. Lastly, *proportionality* represents the substance of PII collected, versus the identified objectives or reasons for collecting the data (Karyda & Gritzalis, 2009).

Fair Information Practices

According to Karyda and Gritzalis, (2009), doubts have arisen regarding whether efforts to enforce Fair Information Practices (FIP), have improved privacy protection. Moreover, Bonner and Chiasson (2005) stated that irrespective of the frequent attempts to address privacy in research, governmental legislation and commercial privacy policies, apprehensions about privacy continue to accelerate. Karyda and Gritzalis, (2009) stated that FIP is comprised of the following:

Notification: user awareness of data collection;

Choice and consent: user determines PII usages, right of access to collected data, protection of data, and the accountability of the collectors of data;

Anonymity and pseudonymity: applies only when identity or privacy is not at risk;

Security and protection: varying levels of privacy protection, dependent on the PII being pursued.

Access and recourse: the ability to know one's PII and to have recourse if violated (FTD, 1998; Karyda & Gritzalis, 2009).

Additionally, thorough analysis of privacy legislation indicates “that the FIP that underlies such legislation paradoxically leads towards reducing privacy, rather than protecting it” (269). This seemingly contradictory statement has been attributed to individuals, rather than society or organizations, exercising greater control over their PII and IOP (Cate, 2006). Thus, this key human element of individual personal responsibility for PII protection and IOP prevention, still in its infancy, is the failure of knowledgeable users to prevent IOP when they know better (Furnell & Clarke, 2012).

A study conducted by Furnell, Bryant, and Phippen (2007), selected 24 Websites to reflect a variety of interests and lifestyles to better understand public attitudes toward online security. From these chosen Websites, 415 users participated through a hosted survey in conjunction with the Trustguide Project (Lacohee, Crane, & Phippen, 2006) to assess security perceptions of UK home users. Furnell et al. (2007) investigated (a) participants' awareness of security threats to IOP, (b) understanding the security safeguards available, (c) utilizing sources of security advice, (d) expectations of support systems, and (e) factors constraining the use of security amongst home users. Furthermore, businesses indicated that they perceived the threat heightened by the lack of public awareness and compromised home system risks as transcending to businesses. With easy financial gain and unhardened targets at home through botnets, spam, and phishing emails, threats to IOP are a significant area of concern for the home user community (Young,

2006). Thus, the insufficient level of PVOP against the risk of IDT for the year 2012, as indicated by Symantec's Internet Security Threat Report, represents an average number of identities exposed per breach of 604,826 (Symantec, 2013). This study followed the examples of Furnell et al. (2007) as a means to measure individuals' perceptions of the risk of IOP and their need to take steps to protect themselves from breaches of PII as a result of IDT incidents.

Authentication Complexity

Furnell et al. (2004) reported on a study of alternative authentication methods. Their study identified infrastructures as a means of coping with the increasing number of password-protected systems. Adding to the growing burden are Websites, resulting in the ever-increasing occurrences of reuse and sharing of password-sensitive authentications. Regardless, security personnel still prefer password and PIN usage as trade-offs, as the number of imposters and false alarm rates are still high. Thus, the responsibility of memorizing, not sharing, multitudes of passwords, and not sharing any with others is not easy, due to their inconvenience. Such issue can result in significant security breaches of PII and in identity theft. Sasse et al. (2001) conducted a study that indicated that with PINs being more difficult for customers to remember than passwords, individuals are resorting back to using date of birth or writing information on paper.

According to Furnell et al. (2004) UA methods that provide lowered IDT occurrences are single-factor authentications, based on something that the user knows (e.g. passwords or PIN), possesses (smart card, token, or RFID device), or is (e.g. a biometric characteristics like fingerprints, eye retina, face, voice, etc.). Multi-factor authentication can be based on any two of these methods combined (Levy & Ramim, 2009; O'Gorman, 2003). Furthermore, Murdoch,

Drimer, Anderson, and Bond (2010) conducted a study that demonstrated that strengths in multi-factor authentication systems indicated a remarkable decline in fraud following compulsory usage after implementation. This decline is significant in that other online banking fraud rose by 55% during the same time period (Gunson et al., 2010). As a result of increased fraud leading to IDT, two-factor authentication use is increasing in the UK within outside vendor use. However, the fraud rate with single-factor authentication, within known banking entities, remains unaffected (Gunson et al., 2010).

Gunson, Marshall, McInnes, and Jack (2011) conducted an experimental study based on usability, to assess users' attitudes towards using an automated telephone service. Methods of user authentication and verification are becoming routinely automated with knowledge-based authentication. According to O'Gorman (2003), knowledge-based methods of authentication are considered very useful in security services. According to Gunson et al. (2011), users are willing to use this method when an environment, such as Internet banking, represents an environment or vendor that is a known factor and considered trustworthy. However, with the complexity of having to remember multiple passwords, security risks have increased. The cognitive load of remembering so many application passwords has led to misuse and reuse issues among users attempting to simplify their authentication efforts (Gunson et al., 2010). However, users within the same banking industry are weary of using outside vendors because of increased security mishaps reported (silicon.com, 2005). The questionnaire utilized in their banking experiment encompassed cognitive issues, differing levels of complexity, system performance, and system performance in comparison to human assistance. Two conclusions were identified: (a) that PIN numbers were preferred by users, but are less secure than voice use, and (b) security held more importance than convenience as multi-method was preferred over single-method authentication

by 67.2%. The results indicated a favorable usability score at or above 5.0 on a seven-point scale for both types of voiceprint use. Therefore, this study followed the examples of Venkatesh, Morris, Davis, G. and Davis, F. (2003) as the measure of individuals' authentication complexity to minimize all difficulties in accessing required resources in public access environments.

Multi-Method Authentication Systems

With increasing demands being placed on the financial service industries, enhanced means of protecting PII through added security measures is being investigated (Hiltgen et al., 2006). According to Weir et al. (2009), mixed methods of identification are referred to as multi-method or two-factor authentication, versus single-factor, and are being tested in varying degrees. Two-factor authentication is comprised of multiple objects such as card readers or tokens represented by 'what you have,' in addition to a multitude of other types of identification. These other identifications refer to passwords/PINs or biometric devices identified as 'personal characteristics.' Some of these recognized biometric traits are voiceprints, facial features, fingerprints, and gait. Additionally, radio frequency identification is increasingly being used in financial transactions through mobile devices.

According to Coventry, De Angeli, and Johnson (2003), gaining secure access to sensitive areas through possession of held objects, knowledge, or physical characteristics has accelerated significantly through a multitude of consumer devices, services, vehicles, and banking interfaces. However, this expansion of methods to gain authentication has resulted in a battle of supremacy between usability, memorability of passwords, securing of PII, and a consideration of multi-method authentication systems (Adams & Chang, 1993; Adams & Sasse, 1999; Levy & Ramim, 2009; Yan, Blackwell, Anderson, & Grant, 2001). According to De Angeli, Coutts, Coventry,

Johnson, Cameron, and Fischer (2002), as well as Dhamija and Perrig (2000), the continual upgrading of mixed methods of password usage impacts the complexity levels of authentication methods. This impact comprises replacing PINs with forms of biometric identification that includes photos and fingerprints (De Angeli, Coutts, Coventry, Johnson, Cameron, & Fischer, 2002; Dhamija, & Perrig, 2000).

Resistance to Using Multi-Method Authentication Systems

According to Coventry et al. (2003), multitudes of studies by National Cash Register (NCR) Self Service Strategic Solutions were conducted to gain a greater understanding of usability and user acceptance of advancing biometric verification methods. Their research was specifically related to verification technology at Automated Teller Machines (ATM) user interfaces. Their results indicated two elements affect how consumers perceive public technology and its benefits: (a) general attitudes viewed as to what consumers think, versus (b) realistic behaviors viewed as to what they actually do. While it appears that people have become more accepting of the use of facial and fingerprint technology for identification, there remains a level of mistrust due to a misunderstanding of biometrics or PIN functionality. These issues influencing consumers' general confidence in biometric technology online is based on (a) little perceived usefulness of biometrics over PINs, (b) difficulty in accepting futuristic technology as dependable, regarding verification, and (c) potential for fraud through misinterpretation of voice, facial features, or fingerprints. Furthermore, research by NCR reported on by Coventry et al. (2003) indicated that refusal to use certain types of biometrics was based on perceived risks from (a) misuse of PII, (b) biometrics data collected, and (c) health concerns associated with iris verification.

According to Huixian and Liaojun (2009), the challenge of providing “privacy protection of biometric data has become a common concern of the public” (p. 295). Therefore, IOP is recognized as a significant influence over the degree of acceptance of biometric-based authentication. Biometric technologies come with an array of problems that are technical, as well as behavioral (Pons & Polak, 2008). These difficulties include data degradation and variances in data recorded. However, resistance to using is “based on attitudes and behaviors related to user acceptance, trust, habits, etc.” (p. 115). As a result of inconsistent attitudes relative to concerns over privacy, storage, protection, and the potential loss of PII, measuring user resistance is a challenging task. This can be attributed to users exhibiting fear, hesitancy, and discomfort over demands to change from current forms of authentication (Pons & Polak, 2008).

Levy and Ramim (2009) conducted a study with a sample size of 100 non-IT students within the context of e-learning courses in a major university in the southeastern U.S. The study’s initial investigation was on the factors that might influence students’ use of multibiometric authentication during e-learning exams. The results of their study demonstrated that “students’ perceived ease-of-use is the second most significant predictor of students’ intention to use multibiometrics during e-learning exams” (p. 390). Furthermore, their study identified the necessity to integrate a multibiometrics approach as current single factor biometric devices don’t provide the level of certainty for all authentication areas of need. Thus, this study followed the examples of Klaus, Wingreen, and Blanton (2010) as it measured individuals’ resistance to using multi-method authentication systems in public access environments, rather than their willingness to protect themselves from a perceived threat of PVOP, IOP, and AC due to breaches in identity theft.

Contributions of this Study

In this chapter, a Conceptual Model was developed by expanding previously limited research of measuring resistance to multi-method authentication by searching the literature for current problems related to IDT and multi-method authentication systems (MMAS), as there appears to be a gap that needs to be filled. Topics were presented to advance the understanding of users' awareness of the threat of the loss of PII due to IDT, the threat of IOP, and the significance of AC. Information gained from this study may lead to the development of methods of authentication for the protection of users' PII. Therefore, additional research into user's PVOP, IOP, AC, and its influence on RMS in public access environments might be warranted (Altinkemer, 2011; Furnell, 2005; Levy & Ramim, 2009; Nandakumar, 2008; Van Hoose, 2008).

Chapter 3

Methodology

Research Design

This study was a predictive study, which attempted to predict the dependent variable of individuals' resistance to using multi-method authentication systems based on the contribution of the independent variables: PVOP, IOP, and AC (See Figure 1). This study used a survey as an instrument for the purpose of collecting data from participants. Multi-Linear Regression (MLR) was used to investigate the contribution of individuals' PVOP, IOP, and AC to their resistance to using multi-method authentication systems in public-access environments. This study was empirical in nature, and collected quantitative data through the use of a Web-enabled survey instrument delivered to participants' e-mail accounts.

The three methods used in this study for multi-method authentication are fingerprint biometric recognition, a form of RFID referred to as "near field communication (NFC)," and password usage. According to Gottschalk (2010), industry trends are moving toward acceptance of fingerprint biometric recognition. Additionally, Gottschalk (2010) stated that RFID communication is a means of identifying a token or receiving device that is held on the person trying to gain access, or who is being tracked in an area of restriction.

The main research question this study addressed was: What is the contribution of individuals' perceptions of the importance of protecting their PII, noted as Perceived Value of Organizational Protection of PII (PVOP), Invasion of Privacy (IOP), Authentication Complexity (AC), and the

interaction on individuals' resistance to using multi-method authentication systems (RMS) in public-access environments.

In addressing the main RQ, this study uncovered 11 specific hypotheses (noted in null form):

H1: *Individuals' Perceived Value of Organizational Protecting PII (PVOP)* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H2: *Invasion of Privacy (IOP)* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H3: *Authentication Complexity (AC)* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H4: There will be no significant interaction effect of *PVOP*, *IOP*, and *AC* on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H5a: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on age (*AGE*).

H5b: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on gender (*GEN*).

H5c: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's degree major (*DM*).

H5d: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on academic level (*AL*).

H5e: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's prior experience with identity theft (*EXP*).

H5f: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's acquaintance experience with identity theft (*EXA*).

H6: There will be no statistically significant differences on *PVOP*, *IOP*, *AC*, and *RMS* based on individuals who have used a multi-method authentication system and those who have not, as well as student and faculty in public-access environments.

Table 1. Summary Table of Authors and Constructs

Constructs	Sources
Personal Value of Organizational Protection Personal Identifying Information (<i>PVOP</i>)	Nosko, Wood, & Molema, 2010 Furnell, Tsaganidi, & Phippen, 2008
Invasion of Privacy (<i>IOP</i>)	Furnell & Clarke, 2012 Furnell, Bryant, & Phippen, 2007
Authentication Complexity (<i>AC</i>)	Furnell, Papadaki, Illingworth, & Reynolds, 2004 Gunson, Marshall, McInnes, & Jack, 2011
Resistance to Using Multi-Method Authentication Systems in Public Access Environments (<i>EXA</i>)	Coventry, De Angeli, & Johnson, 2003 Levy & Ramim, 2009

A survey instrument was created based on validated literature to address the specific research questions and hypotheses noted above. The following sections address these relevant steps and issues: 1) survey instrument creation; 2) reliability and validity issues; 3) identifying the population and sample procedures to be used; 4) conducting a pre-analysis data screening; as well as 5) theoretical model testing.

Instrument Development

Prior literature indicated that it is more advantageous to use previously established measures in IS research than to create new ones (Leidner & Jarvenpaa, 1995). Furthermore, Moore and Benbasat (1991) presented prior research that was recognized as having reliability and validity for development of new research. As a result, this study developed a survey instrument that uses survey items from previous valid research conducted by Cicchetti, Showalter, and Tyrer (1985), Compeau and Higgins (1995), Heissen, (1987), as well as Igbaria and Iivari (1998). Additionally, Likert-type scale response anchors were utilized as identified by Vagias (2006).

The results of the study by Cicchetti et al. (1985) indicated that: (a) the level of joint-probability of agreement exhibited the lowest based on only two categories; (b) reliability reflected increases in relation to the number of categories used; as well as (c) the level of seven indicated the most reliable results, with any contribution above seven being insignificant. Additionally, Verplanken and Orbell (2003) originally conducted four separate studies. They used a seven-point Likert scale for Studies One and Two, while using an 11-point Likert scale for Studies Three and Four. Nevertheless, Miller (1956, p. 4) noted that “psychologists have been using seven-point rating scales for a long time, on the intuitive basis that trying to rate into finer categories does not really add much to the usefulness of the ratings.” Lewis (1993) found that 7-point scales resulted in stronger correlations with t-test results.

A review of valid literature was conducted to select the survey items for measuring PVOP in public access environments. This study followed the studies of Shareef and Kumar (2012) that addressed the issue of identity theft in the use of global and internal measures to address the theft of PII. Some of the internal measures included authentication and address verification technology software techniques (Shareef & Kumar, 2012). As the research is limited for PVOP,

IOP, and AC against resistance, the questions were reviewed for validation by the expert panel. The Likert scale has categories measuring participant responses from ‘1’ - “not important” to ‘7’ - “highly important” (Cicchetti et al., 1985; Vagias, 2006). The specific items numbered PVOP1 – PVOP10 are provided in Appendix A.

A review of literature was conducted to select the survey items to measure IOP in public access environments. Furnell (2008) developed a list of items as pre- and post- workshop surveys that queried students regarding their IOP. A similar list was suggested by Anderson, Durbin, and Salinger (2008), as well as Furnell (2007). The survey items selected were those that are commonly identified as contributing to increased identity theft (Anderson et al., 2008; Furnell et al., 2007). This study followed the studies of Furnell et al. (2007) to measure IOP. The Likert scale has categories measuring participant responses from ‘1’ - “Strongly Disagree” to ‘7’ - “Strongly Agree” (Cicchetti et al., 1985; Vagias, 2006). The specific items numbered IOP1 – IOP6 are provided in Appendix A.

A review of valid literature was conducted to select the survey items to measure AC in public access environments. This study followed the example of Weir et al. (2009), Gunson et al. (2010), and Gunson et al. (2011) to measure users’ AC within public access environments. This study followed the study of Venkatesh, Morris, Davis, G., and Davis, F. (2003) to measure AC. The Likert scale has categories measuring participant responses from ‘1’ - “Strongly Disagree” to ‘7’ - “Strongly Agree” (Cicchetti et al., 1985; Vagias, 2006). The specific items numbered AC1 – AC6 are provided in Appendix A.

An investigation into the relationship between user resistance and mandatory user technology requirements within large scale enterprise systems (ES) was conducted by Klaus, Wingreen, and Blanton (2010). Their study consisted of 186 companies that had implemented an ES against

which little was known of user resistance. Additionally, user resistance was identified as the second highest cost factor related to cost overruns, and the highest barrier to implementation (Cooke & Peterson, 1998). This study followed the studies of Paine, Reips, Stieger, Joinson, and Buchanan (2007); Cases, Fournier, Dubois, and Tanner (2010), as well as Klaus, Wingreen, and Blanton (2010) to measure RMS. The Likert scale has categories measuring participant responses from '1' - "Strongly Disagree" to '7' - "Strongly Agree" (Cicchetti et al., 1985). RMS is using seven items RMS1 to RMS7 as provided in Appendix A. Those scales are (1) strongly disagree, (2) disagree, (3) somewhat disagree, (4) neither disagree nor agree, (5) somewhat agree, (6) agree, and (7) strongly agree.

Straub (1989) stated that different methods of establishing content validity should include literature reviews and expert panels. Furthermore, Sekaran (2003) indicated that content validity "establishes the representative sampling of a whole set of items that measures a concept, and reflects how well the dimensions and elements of the concept have been delineated" (p. 364). The three independent variables, PVOP, IOP, and AC, as well as RMS, the dependent variable, were developed through a review of valid literature. Nevertheless, the variables on the survey instrument have yet to be validated in the context of RMS in public access environments. Therefore, an expert panel was formed to safeguard content validity. The expert panel consisted of terminally degreed experts in the IS field. An anonymous survey was presented to the expert panel members, who were given two weeks to review and comment on the content of the different variables. Once the panel submitted its recommendations, any suggested changes were addressed; the items were resubmitted to the panel for final review and consensus.

A pilot study was conducted, using a small sample of 15 to 25 users including students and instructors, to strengthen the overall instrument validity. According to Trochim and Donnelly

(2008), “measures, samples, and designs don’t have validity—only propositions can be said to be valid (p. 20). Therefore, a measure is what leads to valid conclusions or inferences. Thus, it is a proposition, inference, or conclusion which can have validity” (Trochim & Donnelly, 2008). According to Sekaran (2003), the “reliability of a measure is an indication of the stability and consistency with which the instrument measures the concept and helps to assess the 'goodness' of a measure” (p. 203). As a result, construct validity affirms “how well the results obtained from the use of the measure fit the theories around which the test is designed” (Sekaran, 2003, p. 207).

Following the example of Venkatesh and Morris (2000), as well as Albirini (2006), this study collected the following demographic information from individuals in the sample groups: age, gender, degree major, academic level, prior personal experience with identity theft, and acquaintance experience with identity theft. This information ensured the data collected was representative of the population.

Validity and Reliability

Validity can be defined “as the best available approximation to the truth of a given proposition, inference, or conclusion” (Donnelly & Trochim, 2008, p. 20). Three traditional types of validity are (1) content, (2) criterion-related, such as predictive or concurrent, and (3) construct (Creswell, 2003; Sekaran, 2003). Additionally, validity provides “evidence that the instrument, technique, or process used to measure a concept does indeed measure the intended concept” (Sekaran, 2003, p. 425). Validity is a reflection of the depth of accuracy by which a survey measures the intended item and permits interpretation of the participant scores (Gay, 1996; Litwin, 1995). According to Boudreau, Gefen, and Straub (2004), unbiased observers of a

study consider the prerequisites of relevance and measurability mandatory for obtaining trustworthiness.

Internal validity refers to “whether the observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables” (Straub, 1989, p. 151). Additionally, internal validity is reflective of the trustworthiness or authenticity of the cause-and-effect relationships between two different variables (Sekaran, 2003). According to Creswell (2003), internal validity threats are “experimental procedures, treatments, or experiences of the participants that threaten the researcher’s ability to draw correct inferences from the data in an experiment” (p. 170). This study addressed the research questions using developed measures that have been validated in previous research, along with anonymous measures of individuals’ personal experiences and demographics.

External validity refers to the generalizability of results in various field settings that becomes transferable to entire organizations (Sekaran, 2003). Additionally, external validity refers to the approximate truth of conclusions that involve the generalizability of conclusions for other persons, places, and times (Cook & Campbell, 1979; Shadish, Cook, & Campbell, 2002). One aspect of generalizability, referred to as "proximal similarity," denotes the consideration of differing contexts that are more or less like one's own study (Trochim & Donnelly, 2008). The utilization of random selection and proximal similarity by means of “providing data about the degree of similarity between various groups, places and even times” could significantly enhance generalizability (Trochim & Donnelly, 2008, p. 36). The generalizability of this study was focused on similar organizations, as the individuals in the sample group were expected to number approximately 250, or 40% of the student body, from a small, private university from a single geographic location in the southwestern United States. In addition, individuals with

minimal computer experience may have difficulty using the authentication technology equipment, or resist using the equipment, due to the nature of the technology. Therefore, these factors may reduce the generalizability of the results to other public-access environments and contexts not included in this study sample.

Reliability is defined as the extent to which constructs are free from error, as well as yield results over a specific, consistent time-frame that represent the total population being studied, and to which extent the final results are reproducible under similar methodology (Joppe, 2000; Leedy & Ormrod, 2001; Straub, 1989). Cronbach (1951) developed the measurement, known as Cronbach's Alpha, to establish a means of measuring the internal consistency of a test or scale, with values ranging between 0 and 1.0. The values of .60 to .70 are considered the lower levels of acceptable reliability among the indicators (Geffen, Straub, & Boudreau, 2000). However, Sprinthall (1997) indicated that reliability values above .70 were preferred. Sekaran (2003) identified Cronbach's Alpha as "a reliability coefficient that indicates how well the items in a set are positively correlated to one another" (p. 207). Hair, Anderson, Tatham, and Black (1984) indicated that Cronbach's Alpha is the most commonly used measure of reliability for a set of two or more indicators for constructs. According to Leedy and Ormrod (2001), case studies are required to have a specifically defined time-frame. Furthermore, Kirk and Miller (1986) identified three types of reliability referred to in quantitative research as (1) the extent to which a repeated measurement remains consistent, (2) the stability of a measurement over a specific time-frame, and (3) the similarity of measurements within a specified timeframe. Tavakol and Dennick (2011) defined *internal consistency* as a means by which all items within a construct are measured by the same concept, and are inter-linked with each other. Therefore, *reliability* could be considered the correlation of a construct with its items (Tavakol & Dennick, 2011). Each

construct was measured individually to determine reliability with a Cronbach's Alpha analysis (Levy, 2006; Sprinthall, 1997).

Population and Sample

The sample population in this study were individuals at a small, private university in the southwestern U.S. While the total sample population of participants was approximately 600-700 individuals, participation was expected to be approximately 250 individuals for the research study. The makeup of the student body is approximately 34 years of age with 60% female versus 40% male students. Students attend most classes in the evenings and are considered non-traditional. The breakdown of the sample is such that the control group and the experimental group would each have approximately 125 individuals, reflecting differing degree majors, as well as academic levels. The sample group was further divided by the identifying of each of the participants. The surveys labeled as a) faculty-username/password and c) student-username/password comprised the experimental group. The surveys labeled as b) faculty-multimethod authentication system and d) student-multimethod authentication system comprised the control group. The majority of students are employed and are attempting to further their skill levels, position advancement, as well as, employability through an accredited college. The experimental group received a video training before entering the computer lab. Upon entering, the experimental group received an updated student proximity ID card with RFID technology and provided a fingerprint template. Upon completion of these steps, they were instructed on how to complete the online survey. The control group was instructed to use their pre-existing method of username and password to complete the survey. The control group authentication method was more related to the concerns of users forgetting their passwords,

improper entries, and being locked out occasionally. Password risks are universally recognized patterns that are used in many environments based on all participants using the same identical data for recognition. After completion of the survey, the students received training in the use of the multi-method authentication system based on RFID and biometric identification. The experimental group differed in that they received training in the use of the multi-method authentication system first and then completed the survey. Participants were presented with the biometric and RFID device information through an introductory training class presented to them prior to taking the survey. The participants were tested on their abilities with the specific emerging biometric technology for use in e-commerce authentication in public-access environments. Contact was made with all instructors informing them of the purpose and importance of the survey/study as it relates to their students. Once the survey and study were prepared for deployment, a follow-up visit was made to each instructor to answer any questions and determine if assistance was needed prior to the actual data collection being conducted. The emerging fingerprint biometric and RFID technology that provided the basis for this study were the primary technologies explored.

An online survey instrument was provided through a Web link on each participant's computer provided for the study. The results were tabulated through the Web-based survey instrument. The response data was collected and validated on a centralized system and was safeguarded for accuracy, preventing any alterations of the results.

Pre-Analysis Data Screening

According to Levy (2006), pre-analysis data screening is of critical importance for maintaining accuracy, assuring consistency in or completeness of responses, looking for missing

data, and screening for the extreme multivariate outliers. Thus, the four identified reasons for pre-analysis data screening were: (1) correctness of the data collected, (2) response-set issues, (3) recognizing missing data, and (4) existence of outliers. In this study, the collected survey data was exported to the Statistical Package for the Social Sciences® (SPSS) Statistics 22.0 (SPSS, n.d.) for analysis, after screening for the four areas of critical importance listed above (Mertler & Vannatta, 2010).

The first reason for pre-analysis data screening is to be certain that the accuracy of data collected doesn't improperly influence validity results (Mertler & Vanatta, 2010; Tabachnich & Fidell, 1996). To ensure an accurate data collection process that prevents invalid data results, a Web-based survey instrument was utilized for data collection. This assisted in eliminating errors that might occur through manual data entry of the collected data results; however, additional visual observation of the data was done to ensure data accuracy during the data collection and prevent any data submission and/or Web-based survey instrument errors.

The second reason for pre-analysis data screening is response-set concerns where participants provide the identical answer to all questions on a measureable survey instrument (Levy, 2006). According to Gurwitz (1987), the inclination for participants to provide answers to a survey instrument based on their particular frame of thinking, rather than the actual question being presented, is viewed as a potential response-set worry. Of particular concern is the event where a participant has answered all or nearly all questions with the same score without reading the questions. To address this response-set concern, the study conducted an analysis to consider any response-set removal prior to final analysis.

The third reason for pre-analysis data screening is to avoid the incidence of missing incomplete data that can occur during response times of a survey instrument (Schafer & Olsen,

1998). These can occur when participants “may be unwilling or unable to respond to some items or may fail to complete sections of a [survey instrument] due to lack of time or interest,” (Schafer & Olsen, 1998, p. 545). However, the impact of trying to accommodate these occurrences by deleting or minimizing their contribution to the results can lead to other unpredictable results, thus, influencing outcomes (Hertel, 1976). To minimize this potential problem, the survey instrument needed to be concise with an established completion time-frame during which all questions were to be completed prior to submission. This procedure ensured that all surveys were submitted without missing data. However, the data was observed prior to full analysis to ensure there were no missing data.

The last reason identified by Levy (2006) for pre-analysis data screening is the potential for distortion due to extreme cases, also known as outliers. Hodge and Austin (2004) defined an *outlier* as a participant answer or observation that has deviated notably from what is viewed as the norm of others surveyed. The use of accepted research tools for recognizing outliers is essential to eliminating potential data set corruptors that may threaten validity (Penny, 1996). One such tool for detecting outliers is the Mahalanobis Distance, which was used on the data collected to test for multivariate outliers. Cases that were recognized as multivariate outliers were closely investigated for potential removal prior to further analyses.

Data Analysis

The main research question that this study addressed is: What is the contribution of PVOP, IOP, AC, and their interaction on individual resistance to using multi-method authentication systems in public access environments? To understand further the relative significance of the contribution of the three independent variables (PVOP, IOP, & AC) and their interaction in

predicting RMS in public access environments, a multiple linear regression (MLR) analysis was conducted.

According to Mertler and Vannatta (2010), three statistical tests are used to address the degree of relationship between variables. The three tests are Bivariate Correlation and Regression, Multiple Regression, and Path Analysis. Of these, “Multiple Regression identifies the best combination of predictors (IVs) of the dependent variable” (Mertler & Vanatta, 2010, p. 14). The factors that determine which test to apply to this research were based on the number of independent variables, the categories of the independent variable, and dependent variables (Mertler & Vannatta, 2010). This study used MLR to analyze hypotheses H1 through H4 to determine if a causal relationship exists between users’ PVOP, IOP, AC, and their interaction on RMS. Additionally, a multivariate analysis of covariance (ANCOVA) was used to analyze hypotheses H5a-H5f to determine if a causal relationship exists between users’ PVOP, IOP, AC on RMS when holding the control variables constant (i.e. covariates). The Hypothesis H6 used a t-test to determine if a significant difference existed on the measures of users’ PVOP, IOP, AC, and RMS based on individuals who have used a multi-method authentication system in public-access environments and those who haven’t, as well as the comparisons between student and faculty.

After the pre-analysis data screening, reliability, and validity tests were completed, further statistical analyses were performed. The effects of the independent variables on the dependent variables were investigated by using the MLR model. According to Chen and Hughes (2004), MLR used independent variables to predict the probability of the dependent variable using a linear approach. Thus, MLR was an appropriate starting approach for measuring the effect of the independent variables on the dependent variable in this study (Chen & Hughes, 2004).

According to Sekaran (2003), MLR analysis is defined as “a statistical technique to predict the variance in the dependent variable by testing the independent variables against it” (p. 420). The coefficient significance level was measured to determine whether any of the independent variables were significant. Therefore, the MLR equation for this study consists of three independent variables, one interaction, and one dependent variable. The MLR was completed for each group separately with the same questions being presented to each group. The hypotheses for PVOP, IOP, and AC reflected different responses for those not having been trained first, versus those who received training prior to using the multi-method authentication and then completed the survey. This may indicate that prior training could convince individuals to use the multi-method authentication system.

This study examined a model to test the contribution of three independent variables: PVOP, IOP, and AC, along with their interaction to the dependent variable: RMS. The study followed the example of others (Brady, 2010; Perez, 2013) and used regression analysis to test the strength of the prediction model. According to Mertler and Vannatta (2010), “multiple regression identifies the best combination of predictors (IVs) of the dependent variable” (p. 14).

For MLR, there is a need to aggregate the items within each construct. With a respect to RMS, data aggregation for the purpose of the analyses will be done using a linear summation of the items assessed. The following will represent the data aggregation for the constructs measured:

$$\text{(Eq. 1) } \text{RMS} = \text{RMS1} + \text{RMS2} + \dots + \text{RMS7}$$

$$\text{(Eq. 2) } \text{PVOP} = \text{PVOP1} + \dots + \text{PVOP10}$$

$$\text{(Eq. 3) } \text{IOP} = \text{IOP1} + \text{IOP2} + \dots + \text{IOP6}$$

$$\text{(Eq. 4) } \text{AC} = \text{AC1} + \text{AC2} + \dots + \text{AC6}$$

MLR will investigate the significance and magnitude of the weights (w_1 , w_2 , & w_3)

$$\text{(Eq. 5) RMS} = w_1 * \text{PVOP} + w_2 * \text{IOP} + w_3 * \text{AC} + \text{constant}$$

The results from the data analyses are presented in various tables and figures in the results section of the next chapter. Conclusions were derived from the data reported in the tables and figures and summarized accordingly. The MLR analyses were used to examine the significance of the contribution of the independent variables and their interaction on the dependent variable, and then the results were presented.

Resources Requirements

To conduct the survey, the following resources will be required:

1. NSU dissertation advisor and committee
2. NSU IRB advisor
3. WBU Vice President of External Campuses
4. WBU Dean and Executive Director of Wayland Baptist University-Lubbock
5. WBU expert panel
6. MMAS biometric and smart card readers

Additional testing resources required for this study included biometric fingerprint devices and USB-installed radio frequency identification (RFID) devices for authentication recognition. The devices required software to be installed on each of the test units. The testing labs were isolated computer labs reserved for special activities, to prevent any potential misuse or interference during the testing phase. Access to the participants was managed through the university's communication system. A survey instrument was created for participant use. All required hardware and software resources were installed for the experiment. To ensure the

validity of the testing devices' accuracy and effectiveness, the devices received the required approval from the university. The Web-based survey conducted through the use of the electronic survey software, Google Docs™, undertook pre-analysis, and was analyzed for all statistical techniques using SPSS. The NSU's digital library resources were used throughout this investigation (NSU Libraries, n.d.).

Summary

Chapter three provided the description of the methodology, the research design, and the four survey instruments with their various measures used in this study. This study sought to measure participants' differences in how they valued their organizational protection of personal identifying information, the invasion of their privacy, their level of importance placed on authentication complexity, and how these variables interacted with their level of resistance to using multi-method authentication measures. The developed survey instruments are listed in Appendix A-D of this dissertation. Addressed in this chapter were both internal and external validity and any related issues that required resolution. An expert panel was established to address potential issues such as the scale level and validity of questions, prior to being placed within the Web-based survey (Straub, 1989). Furthermore, the measure of Cronbach's Alpha is necessary to ensure reliability (Sekaran, 2003).

This study addressed issues with reliability associated with raw data being inaccurate, response-set, missing data, and outliers. Furthermore, collinearity, correlation, and covariate reports were examined. The data was analyzed using descriptive statistics for the means and standard deviations. Further, ANCOVA tests for means checked the data for statistical significant differences between the experimental and control groups that represented the four

different survey groups. The surveys labeled as (a) faculty-username/password and (c) student-username/password comprised the experimental group. The surveys labeled as (b) faculty-multimethod authentication system and (d) student-multimethod authentication system comprised the control group. Lastly, resources required for the study were provided.

Chapter 4

Results

Overview

This chapter outlines results of the data analysis for this empirical study. The outcome of the three independent variables, Perceived Value of Organizational Protection of Personal Identifying Information (PVOP), Invasion of Privacy (IOP), and Authentication Complexity (AC), on the singular dependent variable, Resistance to Using Multi-Method Authentication System (RMS), were explored. The results for this study were accomplished in four phases.

Phase I: Exploratory Research, details the development of the four Web-based survey instruments by conducting a thorough literature review based on topics related to constructs in the field of IS related to PII, IOP, AC, identity theft, trust, and resistance to technology usage (Nosko, Wood, & Molema, 2010; Furnell, Papadaki, Illingworth, & Reynolds, 2004). Phase II, the Delphi Method, was used to present the developed instrument to the assembled expert panel for their feedback and adjustments. The Delphi Method employs the use of a multi-iterative approach to construct a consensus forecast based on the key assumption that recommendations from a group of experts that for increased internal validity of the instrument (Okoli & Pawlowski, 2004). Phase III, Pre-Survey Training, details the correct survey selection, training video participation, biometric data collection, and survey instruction. Phase IV, Quantitative Research, specifies the data collection and analysis methods followed. The pre-analysis data screening inspected the results of survey data for accuracy, response-sets, missing data, and

outliers (Ellis & Levy, 2003). Finally, the descriptive statistics examined the data analysis results for PVOP, IOP, AC, and RMS. The Cronbach alpha reliability test, the ANCOVA tests for the covariates, the significance test for differences on the demographic variables, and the t-tests were used to report results.

Phase I: Exploratory Research

Phase I: Exploratory Research, details the development of the Web-based survey instruments based on existing measures in order to collect data for this study. An extensive literature review was conducted in the IS and Web-based systems literature in order to identify the most prevalent issues related to research of multi-method authentication systems. along with the demographic variables that are associated with the potential resistance constructs to such systems. The survey instrument was developed with peer-reviewed journal articles identified as relevant to the topics to be explored from prior studies as listed in Table 1. The demographic variables reflected on the survey instruments were selected based on prior studies related to authentication systems research, which include: age, gender, degree major, academic level, no privacy intrusion, no acquaintance privacy intrusion based on IDT, and password misuse (Coventry, De Angli, & Johnson, 2003; Furnell & Clarke, 2012; Levy & Ramim, 2009; Nosko, Wood, & Molema, 2010). The survey instrument was specifically designed to be used with Google Docs[®], a Web-based survey tool.

Phase II: Delphi Method

Phase II: the Delphi Method, detail the gathering of the expert panel for pre-screening of the preliminary Web-based survey instrument. The expert panel examined the layout, strength of

questions, Likert scale to be used, and validity of the instruments as a whole. The Delphi expert panel consisted of six experts from the IS, mathematics, education, and online-learning fields listed in Table 2.

Table 2. Delphi Panel Experts

Area of Expertise	Number of Experts
Information Systems	3
Mathematics	1
Education	1
Online-Learning	1

Feedback was collected from the expert panel, appraised, and integrated into the survey instruments after a final review was completed. This process increased the validity of the survey instruments in order to ensure a valid response to the measures. Table 3 reflects feedback provided by the expert panel and related adjustments that were made to the survey instrument after the first cycle. The Delphi expert panel method of consensus was unanimous resulting in no further changes after the first cycle.

Table 3. Adjustments to the Survey Instrument Recommended by the Delphi Expert Panel

Change #	Feedback	Adjustments
1.	Use of a five-point scale	Seven-point Likert scale was used for preciseness
2.	Addition of a question related to refusing to use MMAS unless mandatory	A question was added to the survey related to a mandatory requirement of MMAS
3.	Deletion of repetitive questions	Questions were examined and deleted as appropriate

Phase III: Pre-Survey Selection and Training

Phase III: Pre-Survey Selection and Training began with the distribution of an email inviting recipients to participate in the Web-based survey. The invitation was disseminated to more than 650 students and faculty members. A follow-up email was sent two weeks later. Of the 650

invitations to participate, 206 participants responded, representing a 33% response rate. Each participant was randomly assigned to a group; and each group was directed to the appropriate testing area. The four groups identified were Faculty/MMAS and Student/MMAS, or, Faculty/Username+Password and Student/Username+Password. Only the groups identified as MMAS viewed an instructional video before taking the survey. All other participants conducted the survey in a separate classroom without MMAS equipment or training. After MMAS participants completed the video training, their personal biometric and smart card with RFID technology recognition data was configured.

Phase IV: Quantitative Research

Pre-analysis Data Screening

Phase IV: Quantitative Research, introduced the pre-analysis data screening. All questions were required to be answered prior to submitting the completed survey, thereby alleviating the possibility of missing data. None of the questions were open-ended; and the available responses were based on a seven-point Likert-scale. Since selections for each variable were made from a preset scale of values, data accuracy was ensured. Responses to each of the 29 questions were downloaded to an Excel spreadsheet before loading it to SPSS for further analyses.

After exporting the data, the data set was analyzed for any response-set issues reflecting submitted answers being the same. This occurs when any participants select the same scale value to all the construct items being assessed (Levy & Ramim, 2009). After a visual inspection, no cases were removed, thereby representing a 100% acceptance level of the response-set answers, and leaving 206 useful cases for further analyses. However, to ensure the accuracy of the data, the minimum and maximum values for each item was inspected for responses within the

expected value ranges and to ensure the values were not invalidated during the transfer of data between Google Docs and SPSS. All responses were within the acceptable ranges.

The final step for pre-analysis data screening was to identify multivariate outliers by completing a Mahalanobis Distance analysis within SPSS on the survey items of all independent variables. A 95% confidence level was used in order to identify multivariate outliers. These outliers represent patterns of scores that are extreme or irregular in comparison to others. One outlier case was removed from the data set due to Mahalanobis Distance analysis, leaving a total of 205 useful cases available for additional data analyses. Next, the bell-shaped frequency distribution histogram analysis of the variables was performed to provide evidence that the variables PVOP, IOP, AC, and RMS were normally distributed. The analysis found the distribution as linear and distributed, further provide validity for the use of MLR in this case.

In order to demonstrate homogeneity of variance of the dependent variable, a scatter plot analysis was performed visually using a matrix of scatter plots of the residuals versus the predicted values. The residuals were randomly and relatively evenly scattered on either side of their mean (zero) value with respect to the predicted values. This result reflected homogeneity of variance of the dependent variable. MLR analysis also assumes that the relationship between the independent and dependent variables is linear as reflected in the regression analysis; however, this is not always predictable. This linearity can be an upward or downward slope. Linearity implies that the average change in the dependent variable associated with a unit change in the independent variable is constant. In viewing the matrix of the scatter plot, PVOP presents an inversely related linearity in relation to IOP, AC, and RMS.

Descriptive Statistics Data Analysis

To measure the effect of the independent variables, PVOP, IOP, AC, on the dependent variable, RMS, descriptive statistics were used to calculate the means and standard deviations. Descriptive statistics analysis was used to predict the values of normally distributed dependent variables with a correlation to one or more independent variables (Chen & Hughes, 2004; Tabachnik & Fidel, 2007). In this investigation, the residuals, represented by the differences between the predicted and the observed values, were normally distributed (Table 4). The mean values of the independent variables IOP, AC, and the dependent variable, RMS, were between 3.003 to 3.450 indicating a general tendency for the numerically-coded responses to represent a value somewhere between “somewhat disagree to agree” with the items (score = 3) and “neither disagree nor agree” with the items (score = 4). Additionally, the mean value of the independent variable, PVOP, was 6.586 indicating a general tendency for the numerically-coded responses to represent a value somewhere between “very important” with the items (score = 6) and “highly important” with the items (score = 7). The standard deviations of all of the variables ranged from .769 to 1.134, indicating a relatively controlled variability in the responses.

Table 4. Descriptive Statistics (Means and Standard Deviations) (N=205)

	PVOP	IOP	AC	RMS
Mean	6.586	3.056	3.450	3.003
Standard Deviation	.769	1.103	.981	1.134

Tabachnik and Fidell (2007) indicated that collinearity is the inter-correlation between the predicting variables in an MLR model. Therefore, when the inter-correlation is excessive, the standard errors are inflated. This influences the signs and the magnitudes of the regression coefficients. According to Tabachnik and Fidell (2007), this inhibits accurately assessing the relative importance of each of the predicting variables. Collinearity presents a significant

problem when the research methodology is designed to predict the effect of the independent variables on the dependent variable. As demonstrated by O'Brien (2007), evaluating the possibility of excessive collinearity is dependent on the necessity of the researcher's level of rigor. Descriptive statistics did not violate the statistical assumptions of MLR with respect to collinearity as presented in Table 5.

Table 5. Collinearity Statistics to Predict RMS

Model	Dimension	Variance Proportions			
		(Constant)	PVOP	IOP	AC
1	1	.00	.00	.01	.00
	2	.01	.02	.91	.07
	3	.02	.06	.00	.87
	4	.97	.93	.08	.05

a. Dependent Variable: RMS

The Pearson correlation analysis calculates the potential of excessive collinearity (Tabachnik & Fidell, 2007). When the correlation coefficient matrix includes correlations of approximately 0.7 or higher, excessive collinearity may exist (Tabachnik & Fidell, 2007). A second method to evaluate the effect of excessive collinearity is to calculate the variance inflation factor (*VIF*) statistic (O'Brien, 2007). Although *VIF* values are always greater than or equal to 1, the literature does not specify how large *VIF* values should be to impact a dependent variable. According to O'Brien (2007), there are differences between researchers reporting that *VIF* values over 2.5 indicate excessive collinearity, while other researchers would disagree and apply more lenient *VIF* cut-offs of 4.0 or higher for excessive collinearity.

To ensure that excessive collinearity did not compromise the results, the *VIF* cut-off value used in this investigation was 2.5 as prescribed by Alison (1998). According to the Pearson's correlation of coefficients analysis in Table 6, no variables expressed high levels of collinearity

at approximately 0.7 or higher. Furthermore, all the variables were examined for collinearity and identified as exhibiting values of $p < .01$, thus, completing the testing of the fitness of the experimental variables. Therefore, it can be concluded that there is a statistically significant correlation between PVOP, IOP, AC, and RMS as confirmed by the matrix of Pearson correlation of coefficients. Based on the results of the p values from .000 to .003 indicating significance, the null hypotheses H1, H2, H3, H5 (a-d, f), and H6 (a-b) were rejected. The null hypotheses H4 and H5e were not rejected as listed in Table 6.

Table 6. Matrix of Pearson Correlation of Coefficients (N=205)

		PVOP	IOP	AC	RMS	
PVOP	Pearson Correlation	1	-.165*	-.053	-.280	
	Sig. (2-tailed)- PVOP		.018	.449	.000	***
IOP	Pearson Correlation	-.165*	1	.173*	.208	
	Sig. (2-tailed)-IOP	.018		.013	.003	**
AC	Pearson Correlation	-.053	.173*	1	.455**	
	Sig. (2-tailed)-AC	.449	.013		.000	***
RMS	Pearson Correlation	-.280**	.208**	.455**	1	
	Sig. (2-tailed)-RMS	.000	.003	.000		

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

Cronbach's α reliability tests were computed to determine the internal consistency for the survey items PVOP, IOP, AC, and RMS. The final analysis resulted in acceptable reliability scores for each variable according to Cronbach's α value of .70 (Sprinthall, 1997). The remaining internal consistency in order was PVOP ($\alpha = .960$), IOP ($\alpha = .674$), AC ($\alpha = .752$), and RMS ($\alpha = .847$) respectfully. The reliability analysis results for the survey items are presented in Table 7.

Table 7. Cronbach Reliability Analysis (N=205)

Variable	Number of Items	Cronbach's α
PVOP	10	.960
IOP	6	.674
AC	6	.752
RMS	7	.847

The MLR model used in this investigation was:

$$\text{RMS} = \beta_0 + \beta_{\text{PVOP}} * \text{PVOP} + \beta_{\text{IOP}} * \text{IOP} + \beta_{\text{AC}} * \text{AC}$$

where β_0 represents the theoretical predicted value or the intercept of the dependent variable when all the independent variables are zero; and β_{PVOP} , β_{IOP} , and β_{AC} represent the standardized partial regression coefficients for the independent variables. The descriptive statistics analysis calculated by SPSS to predict RMS using standardized coefficients derived from the mean average of the collected survey data is reflected in Table 8.

$$\text{RMS} = 3.356 - .356 * \text{PVOP} + .097 * \text{IOP} + .492 * \text{AC}$$

The value of $p > .05$ that was used to evaluate the t statistics indicated that the intercept was not zero, and that RMS increased in value with respect to IOP, and AC. The value of $p > .05$ used to evaluate the t statistics indicated that the MLR coefficients for IOP were not important indicators of RMS and RMS did not increase significantly with respect to IOP as presented in Table 7.

Table 8. MLR Coefficients to Predict RMS

Model		Unstandardized Coefficients			
		B	Std. Error	t	Sig.
1	(Constant)	3.356	.689	4.872	.000 ***
	PVOP	-.356	.089	-3.990	.000 ***
	IOP	.097	.063	1.536	.126
	AC	.492	.070	7.015	.000 ***

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

The adjusted $R^2 = .271$ presented in Table 9 indicates that the MLR model predicted a moderate proportion of the variance in RMS.

Table 9. Adjusted R^2 and Standard Error to Predict RMS

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	.530 ^a	.281	.271	.96859

a. Predictors: (Constant), AC, PVOP, IOP

b. Dependent Variable: RMS

Table 10 indicates that there is no significant interaction between PVOP, IOP, and AC on RMS. The results indicate an acceptance of the hypothesis H4.

Table 10. ANOVA Interaction Results for PVOP, IOP, AC based on RMS

		df	F	Sig.
PVOP * IOP * AC	Between	190	1.553	.174
	Groups	203		
	Within Groups			

No significant differences were observed based on RMS, $F(df=190)=1.553$, $p=0.174$

RMS = Dependent Variable

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

Demographic Data Analysis

Demographic data related to the variables of age, gender, degree major, academic level, participants' prior experience with identity theft, and participants' acquaintance experience with identity theft was collected from the 205 participants. The ages of most of the participants were between 19 and 49 accounting for 90% of the sample. The demographic analysis conducted in SPSS included a frequency distribution and percentage rate for each item. Table 11 reflects the demographic distribution of the results of the 205 participants based on age (Levy & Ramim, 2009).

Table 11. Descriptive Statistics of Age Groups (N=205)

Item	Frequency	Percentage (%)
Age Faculty		
18 or Under	0	0.0
19-24	2	6.45
25-29	0	0.0
30-34	4	12.90
35-39	1	3.23
40-54	13	41.94
55-59	3	9.68
60 or older	8	25.81

Continued		
Item	Frequency	Percentage (%)
Age Students		
18 or Under	5	2.87
19-24	36	20.69
25-29	35	20.11
30-34	22	12.64
35-39	25	14.37
40-54	47	27.01
55-59	2	1.15
60 or older	2	1.15

The rate of participation from females was 55 versus 150 for males representing a 25% participation as presented in Table 12. A similar distribution of gender frequencies has been in a number of studies on authentication (Furnell, 2005).

Table 12. Descriptive Statistics of Gender (N=205)

Item	Frequency	Percentage (%)
Gender		
Female	55	26.8
Male	150	73.1

The rate of participation from Business, non-degree, and Science represented 84%, while participation by academic levels reflected a rate of 77% by sophomores, juniors, and seniors in Table 13.

Table 13. Descriptive Statistics for Student Degree Major (N=205)

Item	Frequency	Percentage (%)
Degree Major		
Education	19	10.92
Business	59	33.91
Arts	3	1.72
Science	44	25.29
Religion	4	2.30
Other	45	25.86

The demographic data indicated an evenly spread level of participation on the part of sophomore, junior, and senior groups. This group characterized 76.7% of all participants in Table 14.

Table 14. Descriptive Statistics of Student Academic Level (N=205)

Item	Frequency	Percentage (%)
Academic Level		
Freshman	19	10.92
Sophomore	42	24.14
Junior	51	29.31
Senior	39	22.41
Bachelors	10	5.75
Masters	12	6.90
Other	1	.57

The demographic analysis conducted in regards to Participants' Prior Experience with Identity Theft and Participants' Acquaintance Experience with Identity Theft included a frequency distribution and percentage rate for each item. Table 15 reflects the demographic distribution of the results of the 205 respondents based on Participants' Prior Experience with Identity Theft and Participants' Acquaintance Experience with Identity Theft.

Table 15. Descriptive Statistics of Participants' Prior Experience with Identity Theft (N=205)

Item	Frequency	Percentage (%)
Participants' Prior Experience with Identity Theft		
0	103	50.2
1	51	24.9
2-3	39	19.0
4-5	7	3.4
6 or more	5	2.4

The rate of occurrence for Participants' Prior Experience with Identity Theft between zero and three represented 94%. The rate of occurrence for Participants' Acquaintance Experience with Identity Theft between a value of "zero to three" represented 86% in Table 16.

Table 16. Descriptive Statistics of Participants' Acquaintance Experience with Identity Theft (N=205)

Item	Frequency	Percentage (%)
Participants' Acquaintance Experience with Identity Theft		
0	63	30.7
1	36	17.6
2-3	78	38.0
4-5	13	6.3
6 or more	15	7.3

Figure 2. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Age (N=205)

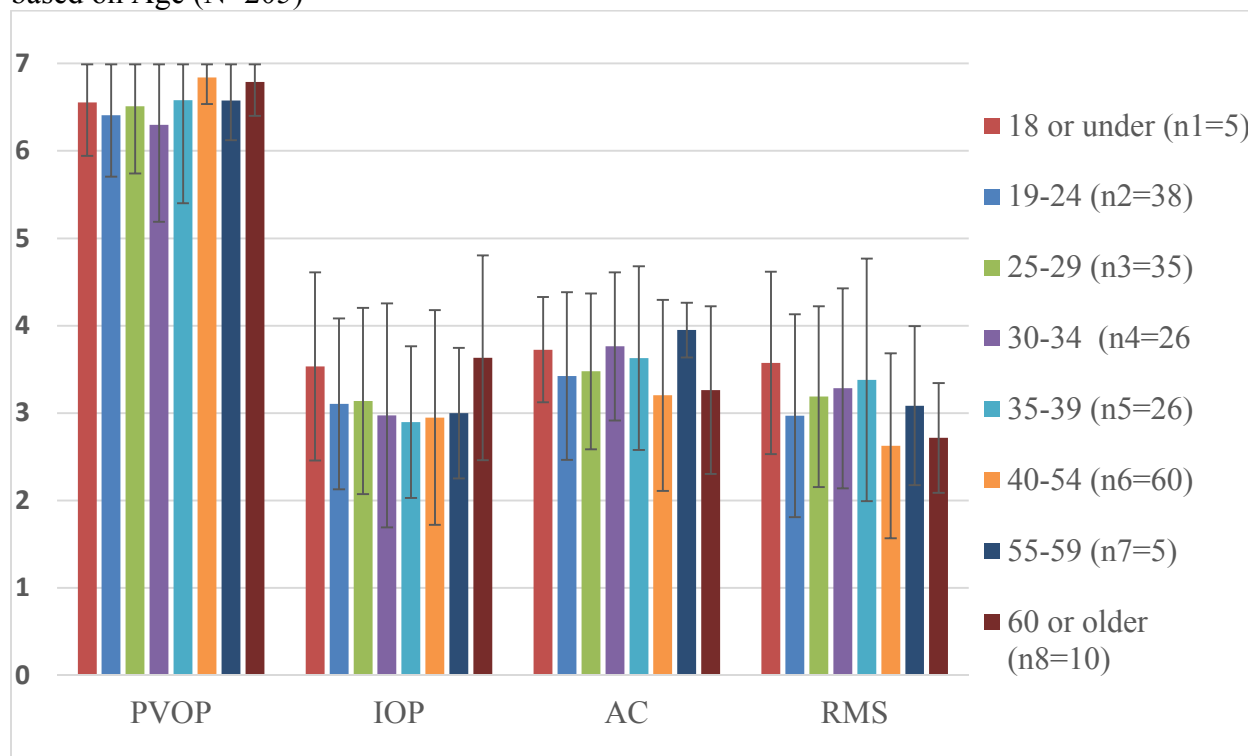


Table 17. ANCOVA Results of PVOP, IOP, AC, and RMS based on Age

		ANCOVA			
		df	F	Sig.	
PVOP	Between Groups	1	1.934	.066	
	Within Groups	197			
No significant differences were observed on PVOP based on Age F(df=197)=1.934, p=0.066					
IOP	Between Groups	1	.735	.643	
	Within Groups	197			
No significant differences were observed on IOP based on Age F(df=197)=.735, p=0.643					
AC	Between Groups	1	1.362	.223	
	Within Groups	197			
No significant differences were observed on AC based on Age F(df=197)=1.362, p=0.223					
RMS	Between Groups	1	2.077	.048	*
	Within Groups	197			
Significant differences were observed on RMS based on Age F(df=197)=2.077, P=0.048					

* - p < 0.05, ** - p < 0.01, *** - p < 0.001

The demographic responses analyzed against PVOP, IOP, AC, and RMS in the observed survey data for Age used an analysis of covariance (ANCOVA). In the ANCOVA, Age was treated as the control variable, which was measured against the mean responses for the 29 questions to see if there were significant differences between the Age groups. Only RMS reflected a statistically significance in Table 17. No other reflected any significant differences.

Figure 3. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Gender (N=205)

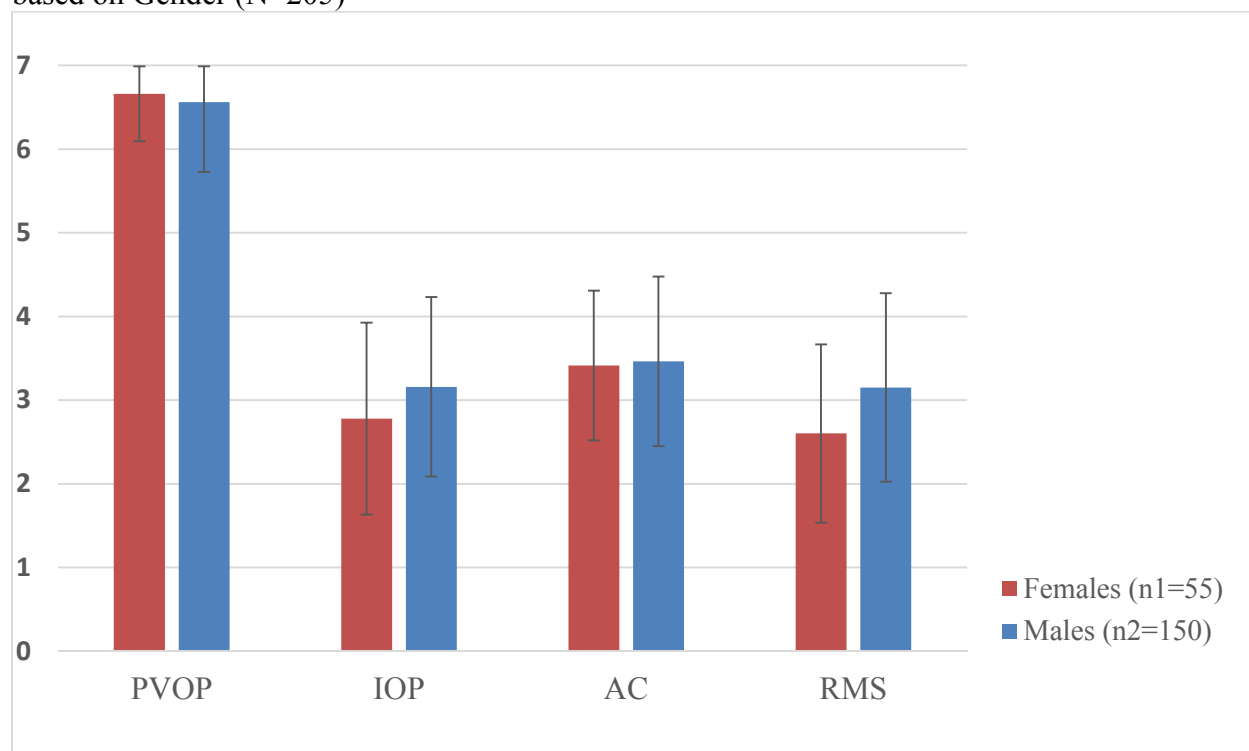


Table 18. ANCOVA Results of PVOP, IOP, AC, and RMS based on Gender

		ANCOVA		
		df	F	Sig.
PVOP	Between Groups	1	.659	.418
	Within Groups	203		
No significant differences were observed on PVOP based on Gender F(df=203)=.659, p=0.418				
IOP	Between Groups	1	4.840	.029 *
	Within Groups	203		
Significant differences were observed on IOP based on Gender F(df=203)=4.840, p=0.029				

Continued					
AC	Between Groups	1	.106	.745	
	Within Groups	203			
No significant differences were observed on AC based on Gender F(df=203)=.106, p=0.745					
RMS	Between Groups	1	9.876	.002	**
	Within Groups	203			
Significant differences were observed on RMS based on Gender F(df=203)=9.876, p=0.002					

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

The demographic responses analyzed against PVOP, IOP, AC, and RMS in the observed survey data for gender used an ANCOVA. In the ANCOVA, Gender was treated as the control variable, which was measured against the mean responses for the 29 questions to see if there were significant differences between the gender groups. Both IOP and RMS reflected a statistically significance difference in Table 17. No other reflected any significant differences.

Figure 4. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, and RMS based on Degree Major (N=205)

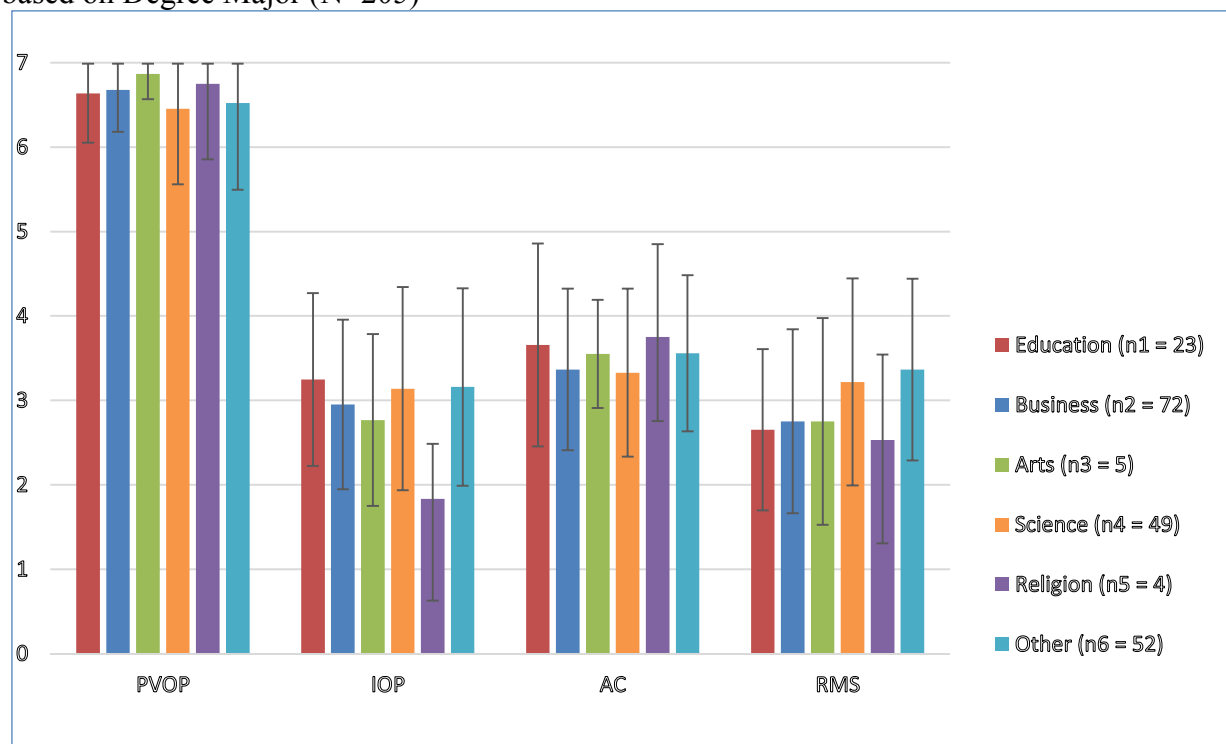


Table 19. ANCOVA Results of PVOP, IOP, AC, and RMS based on Degree Major

		ANCOVA			
		df	F	Sig.	
PVOP	Between Groups	1	.659	.418	
	Within Groups	203			
No significant differences were observed on PVOP based on Degree Major F(df=203)=.659, p=0.418					
IOP	Between Groups	1	4.840	.029	*
	Within Groups	203			
Significant differences were observed on IOP based on Degree Major F(df=203)=4.840, p=0.029					
AC	Between Groups	1	.106	.745	
	Within Groups	203			
No significant differences were observed on AC based on Degree Major F(df=203)=.106, p=0.745					
RMS	Between Groups	1	9.876	.002	**
	Within Groups	203			
Significant differences were observed on RMS based on Degree Major F(df=203)=9.876, p=0.002					

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

The demographic responses analyzed against PVOP, IOP, AC, and RMS in the observed survey data for Degree Major used an ANCOVA. In the ANCOVA, Degree Major was treated as the control variable, which was measured against the mean responses for the 29 questions to see if there were significant differences between the Degree Major groups. Both IOP and RMS reflected a statistically significance difference in Table 19. No other reflected any significant differences.

Figure 5. Analysis Results of Means and Standard Deviations for Academic Level on PVOP, IOP, AC, on RMS (N=205)

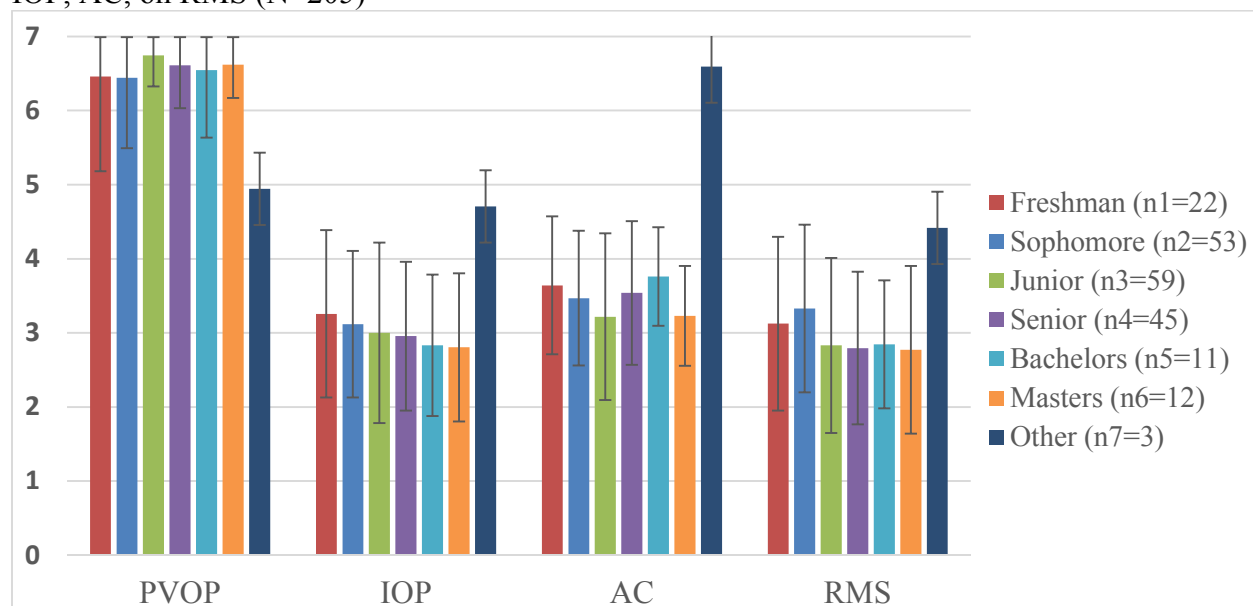


Table 20. ANCOVA Results of PVOP, IOP, AC, and RMS based on Academic Level

		ANCOVA			
		df	F	Sig.	
PVOP	Between Groups	1	.823	.553	
	Within Groups	198			
No significant differences were observed on PVOP based on Academic Level F(df=198)=.823, p=0.553					
IOP	Between Groups	1	1.931	.077	
	Within Groups	198			
No significant differences were observed on IOP based on Academic Level F(df=198)=1.931, p=0.077					
AC	Between Groups	1	1.912	.081	
	Within Groups	198			
No significant differences were observed on AC based on Academic Level F(df=198)=1.912, p=0.081					
RMS	Between Groups	1	2.221	.043	*
	Within Groups	198			
Significant differences were observed on RMS based on Academic Level F(df=198)=2.221, p=0.043					

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

The demographic responses analyzed against PVOP, IOP, AC, and RMS in the observed survey data for academic level used an ANCOVA. In the ANCOVA, Academic Level was treated as the control variable, which was measured against the mean responses for the 29 questions to see if there were significant differences between the academic levels groups. Both IOP and RMS reflected a statistically significance difference in Table 20. No other variables reflected any significant differences.

Figure 6. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, on RMS based on Participants' Prior Experience with Identity Theft (N=205)

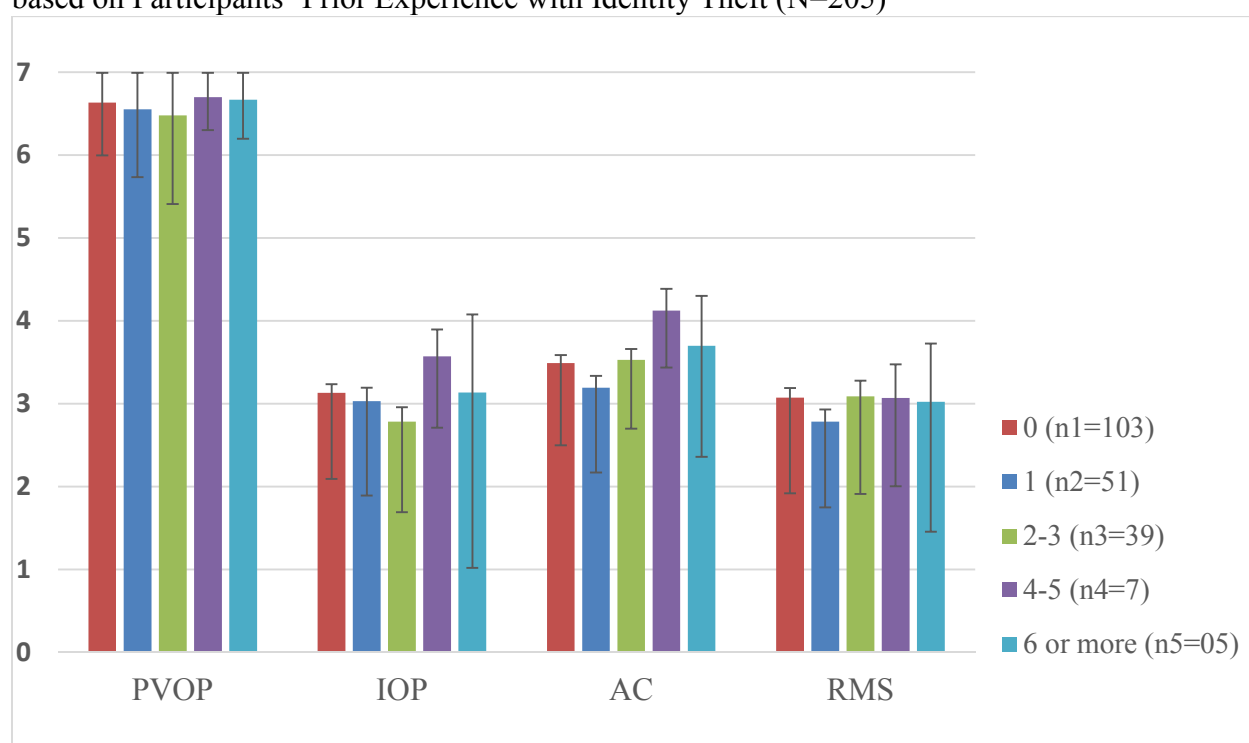


Table 21. ANCOVA Results of PVOP, IOP, AC, and RMS based on Participants' Prior Experience with Identity Theft

		ANCOVA		
		df	F	Sig.
PVOP	Between Groups	1	.359	.838
	Within Groups	200		

No significant differences were observed on PVOP based on Participants' Prior Experience with Identity Theft ($F(df=200)=.359, p=.838$)

Continued

IOP	Between Groups	1	1.122	.347
	Within Groups	200		
No significant differences were observed on IOP based on Participants' Prior Experience with Identity Theft (F(df=200)=1.122, p=.347)				
AC	Between Groups	1	1.920	.109
	Within Groups	200		
No significant differences were observed on AC based on Participants' Prior Experience with Identity Theft (F(df=200)=1.920, p=.109)				
RMS	Between Groups	1	.634	.639
	Within Groups	200		
No significant differences were observed on RMS based on Participants' Prior Experience with Identity Theft (F(df=200)=.634, p=.639)				

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

The demographic responses analyzed against PVOP, IOP, AC, and RMS in the observed survey data for Participants' Prior Experience with Identity Theft used an ANCOVA. In the ANCOVA, Participants' Prior Experience with Identity Theft was treated as the control variable, which was measured against the mean responses for the 29 questions to see if there were significant differences between the Participants' Prior Experience with Identity Theft group. None of the variables displayed any statistically significance difference in Table 21.

Figure 7. Analysis Results of Means and Standard Deviations for PVOP, IOP, AC, RMS based on Participants' Acquaintance Experience with Identity Theft (N=205)

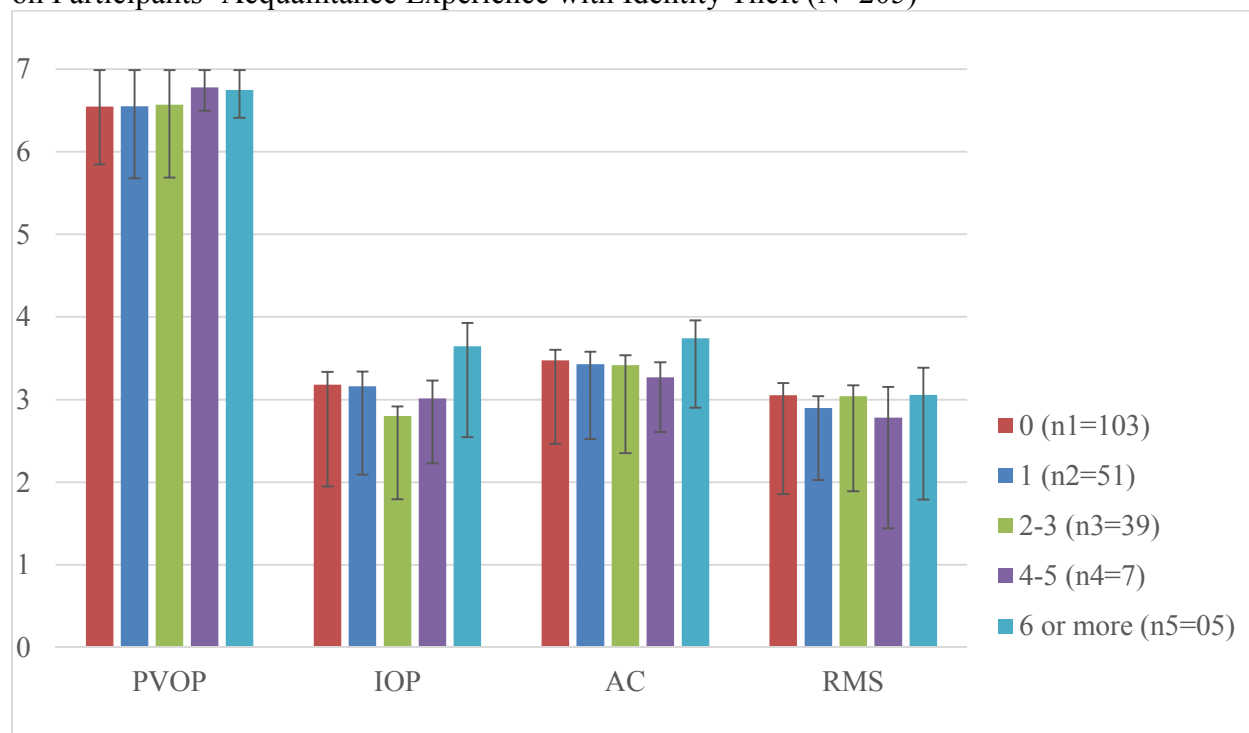


Table 22. ANCOVA Results of PVOP, IOP, AC, and RMS Based on Participants' Acquaintance Prior Experience with Identity Theft

		ANCOVA		
		df	F	Sig.
PVOP	Between Groups	1	.426	.790
	Within Groups	200		
No significant differences were observed on PVOP based on Participants' Acquaintance Prior Experience with Identity Theft (F(df=200)=.426, p=.790)				
IOP	Between Groups	1	2.462	.047
	Within Groups	200		
Significant differences were observed on IOP based on Participants' Acquaintance Prior Experience with Identity Theft (F(df=200)=2.462, p=.047*)				
AC	Between Groups	1	.478	.752
	Within Groups	200		
No significant differences were observed on AC based on Participants' Acquaintance Prior Experience with Identity Theft (F(df=200)=.478, p=.752)				

Continued				
RMS	Between Groups	1	.262	.902
	Within Groups	200		
No significant differences were observed on RMS based on Participants' Acquaintance Prior Experience with Identity Theft (F(df=200)=.262, p=.902)				

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

The demographic responses analyzed against PVOP, IOP, AC, and RMS in the survey data for Participants' acquaintance experience with identity theft used an ANCOVA. In the ANCOVA, Participants' Acquaintance Prior Experience with Identity Theft was treated as the control variable, which was measured against the mean responses for the 29 questions to see if there were significant differences between the Participants' Acquaintance Prior Experience with Identity Theft. IOP was the only variable that displayed any statistically significance difference in Table 21. No other variables reflected any significant differences.

Table 23. T-Test Interaction Results for PVOP, IOP, AC, and RMS based on Student vs. Faculty

		df	F	Sig.	
PVOP	Between Groups	1	.218	.641	
	Within Groups	203			
No significant differences were observed on PVOP based on Student- Faculty (F(df=203)=1.380, p=0.242)					
IOP	Between Groups	1	4.142	.043	*
	Within Groups	203			
Significant differences were observed on IOP based on Student vs Faculty (F(df=203)=.001, p=0.972)					
AC	Between Groups	1	.304	.582	
	Within Groups	203			
No significant differences were observed on AC based on Student vs Faculty (F(df=203)=28.487, p<0.001***)					
RMS	Between Groups	1	1.158	.283	
	Within Groups	203			
No significant differences were observed on RMS based on Student vs Faculty (F(df=203)=9.870, p=0.002***)					

* - $p < 0.05$, ** - $p < 0.01$, *** - $p < 0.001$

Table 23 indicates that there is a statistically significant interaction between IOP on Student vs. Faculty. The results indicate an interaction and rejection of the hypothesis H6.

Table 24. T-Test Interaction Results for Means and Standard Deviation of PVOP, IOP, AC, and RMS based on Student vs. Faculty

		N	Mean	Std. Deviation
PVOP	1.00	174	6.597	.693
	2.00	31	6.526	1.118
IOP	1.00	174	2.990	1.095
	2.00	31	3.424	1.091
AC	1.00	174	3.434	.990
	2.00	31	3.540	.936
RMS	1.00	174	2.967	1.156
	2.00	31	3.205	.990

1.00 (Student), 2.00 (Faculty)

Table 24 indicates the following differences between the means on Student vs Faculty:

PVOP has no significant difference in the means of the two groups.

IOP has the most significant difference in the means of the two groups at .43.

AC has no significant difference in the means of the two groups.

RMS has no significant difference in the means of the two groups at .24.

Table 25. T-Test Interaction Results for PVOP, IOP, AC, and RMS based on MMAS or Not

		df	F	Sig.	
PVOP	Between Groups	1	1.380	.242	
	Within Groups	203			
No significant differences were observed on PVOP based on MMAS or Not (F(df=203)=1.380, p=0.242)					
IOP	Between Groups	1	.001	.972	
	Within Groups	203			
No significant differences were observed on IOP based on MMAS or Not (F(df=203)=.001, p=0.972)					
AC	Between Groups	1	28.487	.000	***
	Within Groups	203			
Significant differences were observed on AC based on MMAS or Not (F(df=203)=28.487, p<0.001****)					
RMS	Between Groups	1	9.870	.002	**
	Within Groups	203			
Significant differences were observed on RMS based on MMAS vs. Not (F(df=203)=9.870, P=0.002)					

* - p < 0.05, ** - p < 0.01, *** - p < 0.001

Table 25 indicates that the t-test Interaction Results for PVOP, IOP, AC, and RMS based on MMAS or Not, reflect a statistically significant difference between AC and RMS. The results indicate a rejection of the hypothesis H6.

Table 26. T-Test Interaction Results for Means and Standard Deviation of PVOP, IOP, AC, and RMS based on MMAS or Not

		N	Mean	Std. Deviation
PVOP	0.00	105	6.524	.928
	1.00	100	6.651	.554
IOP	0.00	105	3.058	1.071
	1.00	100	3.053	1.140
AC	0.00	105	3.785	.929
	1.00	100	3.098	.912
RMS	0.00	105	3.241	1.174
	1.00	100	2.754	1.038

0.00 (NOT), 1.00 (MMAS)

Table 26 indicates the following differences between the means on MMAS or Not:

PVOP has no significant difference in the means of the two groups.

IOP has no significant difference in the means of the two groups.

AC has significant difference in the means of the two groups at .69.

RMS has significant difference in the means of the two groups at .49.

This indicates a very positive response in the use and acceptance of the MMAS authentication method.

Summary of Results

In this chapter, a thorough statistical analysis was conducted based on the data collected from the Web-based survey in order to answer the eleven hypotheses in this study. The detailed methodology consisted of a four phase process for this study. Phase I was an exploratory research of pertinent literature relating to IS, multi-method authentication, identity theft, security, trust, and resistance fields. This information was presented in Table 1 to develop four new

survey instruments adapted from previous studies. Phase II detailed the use of the Delphi Method as presented in Table 2, for implementing an expert panel to present feedback on the validity and reliability of the survey instrument. The results of the expert panel were presented in Table 3 revealing the recommendations and revisions to produce the final survey instruments to collect data for this study. The final survey instruments are found in Appendix A-D. Phase III details the inviting of survey participants, pre-survey selection, video training, and survey instructions that prepared participants for the survey. More than 650 email invitations were disseminated with a response of 206, representing a 33% acceptance rate. Phase IV described the collection, and converting of the data for various forms of analysis.

Upon completion of the pre-analysis data screening, testing for data accuracy, response-set, missing data, and multivariate outliers was completed. Mahalanobis Distance (D^2) values were computed for all 206 cases, with one outlier being identified and removed. The validity and reliability of the survey instruments were measured. Content validity, construct validity, and external validity measures were assured by establishing the survey items on previously validated scales from the literature. Cronbach's α reliability tests were performed for the independent and dependent variables to determine how well the survey items were internally consistent with each other. The results reflected a high internal reliability for the items in each variable. A statistical analyses was performed to confirm that the pre-analysis data screening was done to ensure the accuracy of the data collected from the Web-based survey.

Subsequently, the relevance of the main research question showing the effect of PVOP, IOP, and AC on RMS were presented. To begin with, the data collection procedures were presented, followed by results of the multiple regression analysis. The MLR analysis verified that no variables were collinear. As a result of no collinearity, the MLR model data was presented:

$$\text{RMS} = 3.356 - .356 * \text{PVOP} + .097 * \text{IOP} + .492 * \text{AC}$$

Following the pre-analysis data screening, as well as validity and reliability tests, descriptive statistics for the variables were calculated. These included the mean, standard deviation, and significance. Frequency distribution histograms provided evidence that the variables were normally distributed. MLR and correlation analysis were performed to answer the main research question of the study. Pearson correlation analysis and visual inspection of the matrix of scatter plots indicated that the relationship between the independent variables PVOP, IOP, AC, and dependent variable RMS, were linear, at $p < .01$.

The independent variable IOP was determined not to be statistically significantly related to the dependent variable. This model predicted a moderate proportion of the variance in RMS, reflected by the adjusted $R^2 = .281$. RMS increased significantly at $p < .05$ level with respect to AC and PVOP, while IOP was not a significant predictor of RMS. This model did not violate the statistical assumptions of MLR with respect to residual normality or homogeneity of variance. By comparing the magnitudes of the standardized regression coefficients, AC was recognized as a more significant predictor of RMS than was PVOP or IOP.

Then, the ANOVA test of relevance on the main research question and the hypotheses reflecting the effect of PVOP, IOP, and AC on RMS were presented as not statistically significant. ANCOVA testing was conducted to measure the influence of each of the control variables, “Age, gender, degree major, academic level, Participants’ prior experience with identity theft, and Participants’ acquaintance experience with identity theft” on PVOP, IOP, and AC on RMS. This testing included interaction between the variables and f-tests and their significance. In addition, graphical charts were presented reflecting the levels of means and standard deviations.

According to Shevade and Keerthi (2003) as well as Komarek and Moore (2004), approximately 100 participants are generally required to achieve statistically significant results in regression analysis. The goal of achieving over the minimum level of participation for this study was accomplished with 206 participants, which demonstrated the need for a power analysis was not necessary. This justified the elimination of a power analysis. A summary of the quantitative analysis findings for the research hypotheses are summarized in Table 27.

Table 27. A Summary of the Research Question, Hypotheses, and Findings

Hypotheses	Data Analysis	Findings
MLR Model	Descriptive Statistics of Means and Standard Deviations	Table 4, Page 57 Table 5, Page 58
	MLR Coefficients to Predict RMS Collinearity Statistics to Predict RMS Cronbach, Histogram, Scatter Plot	Table 6, Page 59 Table 7: Page 59 Table 8: Page 58 PVOP $p < .0001$ *** IOP $p = .003$ ** AC $p < .0001$ ***
	Model normally distributed, linear with one response-set removed	MLR Coefficients PVOP $p < .0001$ *** IOP $p < .0001$ *** RMS $p < .0001$ ***
H1 PVOP Research Goal #1	Matrix of Pearson Correlation of Coefficients was used to calculate Significance	Inverse slope Rejected Hypotheses PVOP $p < .0001$ *** IOP $p < .0001$ *** RMS $p < .0001$ *** Table 6, Page 59
H2 IOP Research Goal #2	Matrix of Pearson Correlation of Coefficients was used to calculate Significance	Rejected Hypotheses PVOP $p < .0001$ *** IOP $p < .0001$ *** RMS $p < .0001$ *** Table 6, Page 59

Continued		
H3 AC Research Goal #3	Matrix of Pearson Correlation of Coefficients was used to calculate Significance	Rejected Hypotheses PVOP $p < .0001$ *** IOP $p < .0001$ *** RMS $p < .0001$ *** Table 6, Page 59
H4 RMS Interaction Research Goal #4	ANOVA Test of Between Subject Effects Significance	Not Rejected Hypotheses PVOP*IOP*AC $p = .174$ Not Statistically Significant Table 9, Page 61
H5a Age Research Goal #5	Analysis Results for Means and Standard Deviations of PVOP, IOP, AC, and RMS based on Age ANCOVA Results of PVOP, IOP, AC, and RMS based on Age	Figure 2, Page 63 Rejected Hypotheses RMS $p = .048$ * Table 16, Page 64 18 or under demonstrated highest levels of IOP, AC, and RMS
H5b Gender Research Goal #5	Analysis Results for Means and Standard Deviations of PVOP, IOP, AC, and RMS based on Gender ANCOVA Results of PVOP, IOP, AC, and RMS based on Gender	Figure 3. Page 65 Rejected Hypotheses IOP $p = .029$ * RMS $p = .002$ ** Table 17, Page 65
H5c Degree Major Research Goal #5	Analysis Results for Means and Standard Deviations of PVOP, IOP, AC, and RMS based on Degree Major ANCOVA Results of PVOP, IOP, AC, and RMS based on Degree Major	Figure 4, Page 66 Rejected Hypotheses IOP $p = .029$ * RMS $p = .002$ ** Table 18, Page 66

Continued		
H5d Academic Level Research Goal #5	Analysis Results for Means and Standard Deviations of PVOP, IOP, AC, and RMS based on Academic Level	Figure 5, Page 67
	ANCOVA Results of PVOP, IOP, AC, and RMS based on Academic Level	Rejected Hypotheses RMS $p=.043$ * Table 19, Page 68 Higher levels of education reflected lower RMS Figure 6, Page 69
H5e Participants' Prior Experience with Identity Theft Research Goal #5	Analysis Results for Means and Standard Deviations of PVOP, IOP, AC, and RMS based on Participants' Prior Experience with Identity Theft	
	ANCOVA Results of PVOP, IOP, AC, and RMS based on Participants' Prior Experience with Identity Theft	Not Rejected Hypotheses Not Statistically Significant Table 20, Page 69
H5f Participants' Acquaintance Experience with Identity Theft Research Goal #5	Analysis Results for Means and Standard Deviations of PVOP, IOP, AC, and RMS based on Participants' Acquaintance Experience with Identity Theft	Figure 7, Page 20
	ANCOVA Results of PVOP, IOP, AC, and RMS based on Participants' Acquaintance Prior Experience with Identity	Rejected Hypotheses IOP $p=.047$ * Table 21, Page 71
H6 T-Test Interaction Results for Student vs Faculty Research Goal #6	T-Test Interaction Results for PVOP, IOP, AC, and RMS based on Student vs Faculty	Rejected Hypotheses IOP $p=.043$ * Table 22, Page 72
	T-Test Interaction Results for (Means and Standard Deviations) of PVOP, IOP, AC, and RMS based on Student vs Faculty	Faculty and IOP reflected the highest means Table 23, Page 72

Continued		
H6 T-Test Interaction Results for MMAS or Not Research Goal #6	T-Test Interaction Results for PVOP, IOP, AC, and RMS based on MMAS or Not	Rejected Hypotheses AC $p < .0001$ *** RMS $p = .002$ ** Table 24, Page 73
	T-Test Interaction Results for (Means and Standard Deviations) of PVOP, IOP, AC, and RMS based on MMAS or Not	MMAS displayed lowest levels of AC and RMS Table 25, Page 73

Chapter 5

Conclusion, Implications, Recommendations, and Summary

Overview

In this chapter, conclusions are suggested and discussed based upon the analysis performed within this study. The hypotheses are examined in context of the results achieved along with any limitations of this study. The implications for the study and the contribution to the body of knowledge within the IS field of study related to multi-method authentication is discussed, as well as recommendations for future research. Finally, a summary concludes this chapter of the study.

Conclusion and Summary of Results

To reiterate, the research problem investigated was identity-theft (IDT) incidents due to breaches of personal identifying information (PII) (Venkatesh, Morris, Davis, & Davis, 2003; Zviran & Erlich, 2006). Such PII breaches are significant threats to invasion of privacy (IOP) during e-commerce activities by users in public-access environments (Venkatesh et al., 2003; Zviran & Erlich, 2006). Kim, Jeong, Kim, and So (2011) identified PII as financial card numbers, usernames, passwords, medical records, driver's licenses, and Social Security numbers (Kim et al., 2011). These PII represent targets of online theft during e-commerce activities.

Resistance to using multi-factor authentication is related to the issue of identity theft due to contributing factors of inadequate user authentication (UA) methods (Fichtman, 2001). A

national survey conducted by Information Security Education Journal Volume 1 Number 1 March 2014 the Federal Trade Commission (FTC) (2008) revealed that 4.7% of American adults experienced identity theft that involved the loss of personal identifying information (PII), while such numbers appear to grow rapidly every year. Industry responses to combat the aspects of identity theft are focused on the verifiable identification of individuals through the development of acceptable multi-method authentication systems (Bellah, 2001). While current research has shown significant advances in biometric recognition, users continue to resist using biometric technology to enhance password security including in institutions of higher-education (Levy & Ramim, 2009). This resistance is attributed to concerns related to protecting their PII, invasion of privacy (IOP), and authentication complexity (AC).

The main goal of this proposed research study was to assess empirically individuals' perspectives on the contribution of perceived value of organizational protection of their personal identifying information (PII) (PVOP), perceived invasion of privacy (IOP), and authentication complexity (AC) on their resistance to using multi-method authentication systems (RMS) in public-access environments. The main goal that this research study assessed empirically was individuals' perspectives on the contribution of perceived value of organizational protecting of personal identifying information (PII) (PVOP), perceived invasion of privacy (IOP), and authentication complexity (AC) on their resistance to using multi-method authentication systems (RMS) in public-access environments. To empirically assess the effect of the aforementioned variables on individual acceptance of multi-method forms of access authentication in public access environments, four Web-based surveys were developed using previously validated scales.

The target populations of this investigation were faculty and the entire student body of a small university on southwestern United States. These groups affected various age, gender,

degree majors, and academic levels, Participants' prior experience with identity theft and Participants' acquaintance experience with identity theft. This resulted in an available participation level of 206 participants or 33% response rate. After completing the survey and data collection, a careful MLR analysis demonstrated that the theoretical model of this investigation predicted RMS 97% of the time. Pearson correlation analysis revealed that PVOP, IOP, AC, and RMS were not collinear.

The main research question (RQ) that this study addressed was: What is the contribution of PVOP, IOP, AC, and interaction on individuals' resistance to using multi-method authentication systems in public-access environments?

According to Levy and Ramim (2009), the acceptance of multi-method authentication systems has been applied minimally in the fields of IDT. Additionally, Furnell and Clarke (2012) indicated that personal information security research in human aspects of security has not been applied efficiently in various public environments. Therefore, this investigation identified a new construct: PVOP, IOP, AC, and its effect on RMS, as well as its potential to impact the current ongoing levels of IDT in public access environments. The findings of MLR and correlation analyses demonstrated that PVOP, IOP, and AC, when associated with the covariates, had varying weights in predicting RMS. The findings empirically reaffirm the research reported in the literature by Levy and Ramim (2009) that AC is a significant construct that affects RMS in public access environments.

The findings of MLR and correlation analyses indicated that IOP did not have a strong weight in predicting RMS. Although the findings reported in the literature by Levy and Ramim (2009) asserted that AC is a significant construct that affects RMS, the findings provide additional evidence that more research on the factors associated with RMS is warranted. Based

on the empirically-validated conceptual model of the relevant factors and their effects on RMS, the implications of this investigation for research are significant. The developed theoretical model used the variables of PVOP, IOP, and AC to predict RMS, as well as acceptance of multi-method authentication systems in public access environments. The independent (PVOP, IOP, & AC) and dependent (RMS) variables selected for the model were based on a comprehensive literature search. As a result, the two main contributions that this investigation makes to the IS literature include: (a) the development and empirical validation of a theoretical model for predicting RMS in public access environments, and (b) the determination of the most significant factors that affect RMS in public access environments. These findings should facilitate the understanding of RMS among users of technology in public access environments.

Implications

The implications of this investigation are threefold. First, the results of this study provide guidance for individuals and organizations associated with all methods of authentication in the public access domain. The findings contribute knowledge that can be applied to lower user resistance to MMAS, as well as to reduce incidences of IDT, user access misuse, and organizational failures to protect PII. Second, this investigation provides information that is valuable in understanding RMS, that can be used to (a) decrease personal data security breaches; (b) improve the level of acceptance of biometrics/smart card use in public access environments; (c) prepare through available education and training, for the anticipated changes in MMAS resulting from technological advances; and (d) improve compliance with new federal regulations that mandate different types of authentication in public access environments. Finally, the research model developed as an outcome of this investigation can help MMAS developers

understand the variety of factors especially related to authentication complexity and educating users on how the use and benefits of MMAS affect the current levels of resistance. Based on this study, as well as the existing body of knowledge, users of differing methods of logon identification will better understand how to protect themselves and their clients PII from IDT.

Limitations

In this study, four limitations were identified. First, the participants of this study were identified with a university in a student or instructional role. Therefore, the generalizability of this investigation might be limited to university academic environments. Additional studies need to be done in non-university environments to be able to more broadly generalize the findings of this study. Second, the survey for this investigation was completed within a 3-month time period. A more lengthy longitudinal study might be needed to measure the effect of MMAS training to decrease RMS. Furthermore, MMAS must periodically reassess their methods by minimizing the complexity of devices through the use of more mobile devices as a form of identity recognition.

Third, the data collected was self-reported. Therefore, the reliability of the survey data was dependent on the participants' willingness to report their resistance of MMAS without bias. However, the survey responses were checked for data accuracy, response-set, missing data, and outliers to reduce the self-report bias.

Finally, the Web-based survey instrument invitation was disseminated to the participants through e-mail, with no special incentive given to complete the survey. To increase the response rate, the survey deadline was extended. In addition, two reminders to complete the survey were e-mailed to students, faculty and staff. The professors' willingness to allow students to participate, as well as the participants' willingness to self-select and dedicate the time necessary

to complete the survey, may have contributed to the number of surveys completed. Based on this self-selection, there may have been an under-representation of student and faculty professionals who are not concerned about MMAS or IDT in public access environments.

Recommendations

Several areas of future research were identified. The current study was restricted to one type of survey per participant; and the participant self-selected which instrument to answer. Future studies could also explore whether mandatory MMAS for access into a supermarket for shopping might have a significant response based on improving the knowledge levels of MMAS for future end-users. In addition, researching the perceptions of resistance to MMAS from a broader group of public environments (e.g. supermarkets, sports events, concerts, national borders, churches, movie theaters, & government buildings) within a single community would provide a richer view of differences in MMAS usage and lower RMS within public access environments.

Testing future participants' knowledge of their universities' information security programs could be required in subsequent studies. However, the current study assumed that the participants had an acceptable and working understanding of their personal university logon method requirements. Replicating this investigation to include a wider range of environments that are not included in universities (e.g. government, hospitals, & general public access environments) would increase the generalizability of the findings.

Examining additional factors affecting resistance to MMAS usage from the literature, such as IDT based on culture (Levy & Ramim, 2009), resistance to change (Smith & Jamieson, 2006), and trust (Kim & Ahn, 2007), could also be considered in future research. To ensure that the present study remained controllable, these additional variables were not investigated. Therefore,

this investigation was not an exhaustive study of all factors that affect RMS. This study examined the effect of the independent variables, PVOP, IOP, and AC on the dependent variable, RMS, in public access environments. However, mandatory use of MMAS was not measured. Future investigations could measure actual mandatory use of MMAS in public access environments.

Finally, the results of this investigation indicated that RMS in public access environments represented in part by the university participants, acknowledged that PVOP, IOP, and AC are important factors in achieving reduced MMAS resistance. The literature has reported that individuals are not fully complying with the recommended practices for protecting their PII during logon activities. Thus, an improved understanding of the importance of protecting PII, preventing IOP, and continuing improvement in the reliability of biometric and RFID devices to lower access complexity is suggested. Future research examining factors affecting PVOP, IOP, and AC could result in knowledge to help ensure curbing of MMAS resistance in public access environments.

Summary

This investigation addressed the research problem that individuals in the U.S. are not fully complying with recommended PII behaviors (Furnell & Clarke, 2010; Levy & Ramim, 2009). According to Furnell (2009), data security breaches in annual IDT theft reports continue to increase. Numerous security, corporate, and government organizations have recently reported data security breaches (DataLossDB, 2010; Privacy Rights Clearinghouse, 2010). Furthermore, the rapid growth and use of wireless information technology has created new security issues (Connell & Young, 2007; Helms et al., 2008; Thomas & Botha, 2007). Increasing shortcomings

in PII security related to government, businesses like Target[®], and PayPal[®], as well as, individuals cell phone usage, breach notifications, data transmission standards, investigation of complaints, penalties, and enforcement have created liabilities for numerous organizations (Brown, 2009a, 2009b; Blades, 2009). As a result of these breaches of PII, Hourihan (2009) and Ruzic (2009) indicated that numerous federal, government, banking, academic, medical institutions, and corporations have instituted stronger cyber-security compliance measures.

In conclusion, recent announcements by governments and the banking industry, indicated a plan for development and rollout of a new form of authentication utilizing both hand as well as forehead authentication starting in the year of 2017 (Dykes, 2016). Moreover, recently it was announced that Japan would begin to authenticate with fingerprints as currency for ATM use (The Yomiuri Shimbun, 2016). These efforts to minimize IDT may possibly experience forms of resistance due to uncertainty over fears of IOP, PVOP, and AC, however, as this study indicates, education, and usage with an MMAS method of use with both fingerprint and RFID may lower RMS due to a more acceptable form of AC in public access environments.

Based on a comprehensive review of the literature of PVOP, IOP, and AC, a theoretical model was developed to predict whether any of the three IV has any statistically significant influence on individuals' RMS in public access environments. The goal of the study was to develop a conceptual model, as presented in Figure 1, based on the analysis of the effect of PVOP, IOP, AC, and RMS. The main research question (RQ) that this study addressed was: What is the contribution of PVOP, IOP, AC, and interaction on individuals' resistance to using multi-method authentication systems in public-access environments?

The target sample population of this investigation was student, instructors, and staff associated with a university. In this study, a 29-item Web-based survey was developed with

seven-point Likert-scaled multiple items to determine the factors affecting RMS. The survey was developed using a combination of existing and validated scales. The 10 items for PVOP in the instrument, PVOP1 to PVOP10, were adapted from the survey items developed and validated by Knapp et al. (2007); and six items for IOP support in the instrument, IOP1 to IOP6, were adapted from the survey items developed and validated by Lin (2007). Six items for AC in the instrument, AC1 to AC6, were developed by consolidating and adapting survey items developed and validated by D'Arcy and Hovav (2009); seven items for RMS in the instrument, RMS1 to RMS7, were developed by consolidating and adapting survey items developed and validated by Knapp et al. (2007).

Numerous statistical methods, MLR, ANOVA, ANCOVA, t-test, correlation analysis, collinearity, Cronbach, Histograms, Normality, Mahalanobis, Outliers, and Scatter Plots were used to test the assumptions as well as the conceptual research model of this investigation. The theoretical model predicted that AC would have the most significant effect on RMS and, therefore, reduce IDT. A total of 205 qualified participants participated in the Web-based survey, representing a 33% response rate. Therefore, the results of the investigation demonstrated that AC and PVOP were significant predictors of the dependent variable RMS in the MLR model. IOP was not as significant a predictor of the dependent variable. MLR analysis indicated that the AC independent variable was the most significant predictor of RMS rather than PVOP or IOP.

A power analysis was not performed to validate as the sample size of 205 used in this investigation was adequate to reject the null hypothesis of MLR. Following MLR analysis, the results of the investigation were reviewed. Conclusions were discussed and correlated to PVOP, IOP, AC, and RMS in regards to technology acceptance and reducing identity theft. Theoretical and practical implications of the study were defined. Four limitations of the investigation were

identified and summarized. In conclusion, recommendations were presented for future research that will build upon the research and extend the body of knowledge in the area of RMS in public access areas.

Appendix A

Survey Instrument for User of Multi-Method Authentication - Faculty-Multi-Method Authentication Systems

Dear Participant,

You are invited to take part in a survey regarding multi-method authentication systems for use in public access environments. The purpose of this study is to measure your overall perceptions of using multi-method forms of authentication for security while conducting e-commerce activities in public access environments. Your participation in this survey is voluntary and completely anonymous. Responding and submitting your responses to the survey questions indicates voluntary participation in the study.

The survey should take between 15 to 25 minutes to complete. All responses will be kept confidential. Your survey response is vital to the improvement of reducing identity theft and protecting your personal identifying information by reducing invasion of your privacy through a more efficient means of authenticating your access methods. Thank you for your interest and participation in this survey.

Sincerely,
Joseph Marnell, Ph.D. Candidate
Nova Southeastern University
Graduate School of Computer & Information Sciences

Section A. Perceived Value of Organizational Protection (PVOP) of Personal Identifying Information (PII)

Please rate the level of importance you feel about the following statements from (1) Not Important to (7) Extremely Important in regards to having the university protecting your **Personal Identifying Information (PII)**

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP1: Preventing unauthorized access to your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP2: Prevent theft of your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP3: Prevent the use of your PII without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP4: Prevent the collection of your PII during online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP5: Prevent the interception of your online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP6: Prevent the ability of university personnel to manipulate or change your PII on the university information systems without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP7: Prevent the ability of university personnel to preserve your online transaction PII for their personal interest without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP8: Prevent Internet hackers from having access into your PII on the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP9: Prevent Internet hackers from theft of your PII from the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP10: Prevent Internet hackers from having the ability to intercept, hide, or manipulate some part of your PII from the university's information systems	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Section B. Invasion of Privacy (IOP)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university protect you from ***Invasion of Privacy (IOP)***

Items	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP1: Protecting my personal data isn't my responsibility	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP2: I will not use university systems for registration because of privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP3: Securing my privacy impedes use of my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP4: I don't have time to deal with privacy issues	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
IOP5: I don't know how to secure my information on my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP6: I don't understand the privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section C. Authentication Complexity (AC)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university provide ***multi-method authentication systems (MMAS)*** with minimal ***Authentication Complexity (AC)***

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
AC1: MMAS is more complex to use than previous forms of password identification	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC2: MMAS requires too much time for log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC:3 There are too many MMAS devices required to use	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC4: MMAS would require me to carry additional identification with me at all times to log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC5: MMAS are not accurate enough	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC6: MMAS is more complex than just facial recognition	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section D. Resistance to using multi-method authentication system (RMS)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to your resistance to using *multi-method authentication systems (MMAS)* for university identification

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
RMS1: I am opposed due to MMAS requiring skill changes	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS2: I am opposed to using any MMAS	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS3: I prefer my previous authentication methods as it is easier	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS4: I am opposed to MMAS to protect my PII	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS5: I am opposed to using MMAS due to process uncertainty	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS6: I am opposed to using MMAS due to privacy concerns	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS7: My opposition to MMAS will influence my attendance of the university	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section E. Demographic information.

Gender: Male Female
Age: 18 or under 19-24 25-29 30-34
 35-39 40-54 55-59 60 or older

Degree Major Education Business Arts Science
 Religion Mathematics Other

Academic Level Freshman Sophomore Junior Senior
 Bachelors Masters Other

How man incidents of any form of privacy intrusion or identity theft have you experienced?
 0 1 2-3 4-5 6 or more

How man incidents of any form of privacy intrusion or identity theft has anyone in your family,
at work, school, or an acquaintance experienced?
 0 1 2-3 4-5 6 or more

Appendix B

Survey Instrument for User of Multi-Method Authentication - Faculty-User/Password Method

Dear Participant,

You are invited to take part in a survey regarding multi-method authentication systems for use in public access environments. The purpose of this study is to measure your overall perceptions of using multi-method forms of authentication for security while conducting e-commerce activities in public access environments. Your participation in this survey is voluntary and completely anonymous. Responding and submitting your responses to the survey questions indicates voluntary participation in the study.

The survey should take between 15 to 25 minutes to complete. All responses will be kept confidential. Your survey response is vital to the improvement of reducing identity theft and protecting your personal identifying information by reducing invasion of your privacy through a more efficient means of authenticating your access methods. Thank you for your interest and participation in this survey.

Sincerely,
Joseph Marnell, Ph.D. Candidate
Nova Southeastern University
Graduate School of Computer & Information Sciences

Section A. Perceived Value of Organizational Protection (PVOP) of Personal Identifying Information (PII)

Please rate the level of importance you feel about the following statements from (1) Not Important to (7) Extremely Important in regards to having the university protecting your **Personal Identifying Information (PII)**

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP1: Preventing unauthorized access to your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP2: Prevent theft of your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP3: Prevent the use of your PII without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP4: Prevent the collection of your PII during online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP5: Prevent the interception of your online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP6: Prevent the ability of university personnel to manipulate or change your PII on the university information systems without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP7: Prevent the ability of university personnel to preserve your online transaction PII for their personal interest without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP8: Prevent Internet hackers from having access into your PII on the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP9: Prevent Internet hackers from theft of your PII from the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP10: Prevent Internet hackers from having the ability to intercept, hide, or manipulate some part of your PII from the university's information systems	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Section B. Invasion of Privacy (IOP)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university protect you from *Invasion of Privacy (IOP)*

Items	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP1: Protecting my personal data isn't my responsibility	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP2: I will not use university systems for registration because of privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP3: Securing my privacy impedes use of my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP4: I don't have time to deal with privacy issues	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
IOP5: I don't know how to secure my information on my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP6: I don't understand the privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section C. Authentication Complexity (AC)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university provide ***multi-method authentication systems (MMAS)*** with minimal ***Authentication Complexity (AC)***

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
AC1: MMAS is more complex to use than previous forms of password identification	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC2: MMAS requires too much time for log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC3: There are too many MMAS devices required to use	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC4: MMAS would require me to carry additional identification with me at all times to log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC5: MMAS are not accurate enough	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC6: MMAS is more complex than just facial recognition	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section D. Resistance to using multi-method authentication system (RMS)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to your resistance to using *multi-method authentication systems (MMAS)* for university identification

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
RMS1: I am opposed due to MMAS requiring skill changes	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS2: I am opposed to using any MMAS	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS3: I prefer my previous authentication methods as it is easier	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS4: I am opposed to MMAS to protect my PII	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS5: I am opposed to using MMAS due to process uncertainty	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS6: I am opposed to using MMAS due to privacy concerns	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS7: My opposition to MMAS will influence my attendance of the university	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section E. Demographic information.

Gender: Male Female
Age: 18 or under 19-24 25-29 30-34
 35-39 40-54 55-59 60 or older

Degree Major Education Business Arts Science
 Religion Mathematics Other

Academic Level Freshman Sophomore Junior Senior
 Bachelors Masters Other

How many incidents of any form of privacy intrusion or identity theft have you experienced?
 0 1 2-3 4-5 6 or more

How many incidents of any form of privacy intrusion or identity theft has anyone in your family,
at work, school, or an acquaintance experienced?
 0 1 2-3 4-5 6 or more

Appendix C

Survey Instrument for User of Multi-Method Authentication – Student-Multi-Method Authentication Systems

Dear Participant,

You are invited to take part in a survey regarding multi-method authentication systems for use in public access environments. The purpose of this study is to measure your overall perceptions of using multi-method forms of authentication for security while conducting e-commerce activities in public access environments. Your participation in this survey is voluntary and completely anonymous. Responding and submitting your responses to the survey questions indicates voluntary participation in the study.

The survey should take between 15 to 25 minutes to complete. All responses will be kept confidential. Your survey response is vital to the improvement of reducing identity theft and protecting your personal identifying information by reducing invasion of your privacy through a more efficient means of authenticating your access methods. Thank you for your interest and participation in this survey.

Sincerely,
Joseph Marnell, Ph.D. Candidate
Nova Southeastern University
Graduate School of Computer & Information Sciences

Section A. Perceived Value of Organizational Protection (PVOP) of Personal Identifying Information (PII)

Please rate the level of importance you feel about the following statements from (1) Not Important to (7) Extremely Important in regards to having the university protecting your **Personal Identifying Information (PII)**

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP1: Preventing unauthorized access to your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP2: Prevent theft of your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP3: Prevent the use of your PII without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP4: Prevent the collection of your PII during online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP5: Prevent the interception of your online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP6: Prevent the ability of university personnel to manipulate or change your PII on the university information systems without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP7: Prevent the ability of university personnel to preserve your online transaction PII for their personal interest without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP8: Prevent Internet hackers from having access into your PII on the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP9: Prevent Internet hackers from theft of your PII from the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP10: Prevent Internet hackers from having the ability to intercept, hide, or manipulate some part of your PII from the university's information systems	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Section B. Invasion of Privacy (IOP)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university protect you from ***Invasion of Privacy (IOP)***

Items	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP1: Protecting my personal data isn't my responsibility	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP2: I will not use university systems for registration because of privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP3: Securing my privacy impedes use of my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP4: I don't have time to deal with privacy issues	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
IOP5: I don't know how to secure my information on my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP6: I don't understand the privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section C. Authentication Complexity (AC)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university provide ***multi-method authentication systems (MMAS)*** with minimal ***Authentication Complexity (AC)***

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
AC1: MMAS is more complex to use than previous forms of password identification	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC2: MMAS requires too much time for log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC:3 There are too many MMAS devices required to use	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC4: MMAS would require me to carry additional identification with me at all times to log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC5: MMAS are not accurate enough	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC6: MMAS is more complex than just facial recognition	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section D. Resistance to using multi-method authentication system (RMS)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to your resistance to using *multi-method authentication systems (MMAS)* for university identification

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
RMS1: I am opposed due to MMAS requiring skill changes	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS2: I am opposed to using any MMAS	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS3: I prefer my previous authentication methods as it is easier	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS4: I am opposed to MMAS to protect my PII	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS5: I am opposed to using MMAS due to process uncertainty	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS6: I am opposed to using MMAS due to privacy concerns	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS7: My opposition to MMAS will influence my attendance of the university	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section E. Demographic information.

Gender: Male Female
Age: 18 or under 19-24 25-29 30-34
 35-39 40-54 55-59 60 or older

Degree Major Education Business Arts Science
 Religion Mathematics Other

Academic Level Freshman Sophomore Junior Senior
 Bachelors Masters Other

How many incidents of any form of privacy intrusion or identity theft have you experienced?
 0 1 2-3 4-5 6 or more

How many incidents of any form of privacy intrusion or identity theft has anyone in your family,
at work, school, or an acquaintance experienced?
 0 1 2-3 4-5 6 or more

Appendix D

Survey Instrument for User of Multi-Method Authentication - Student-Username/Password Method

Dear Participant,

You are invited to take part in a survey regarding multi-method authentication systems for use in public access environments. The purpose of this study is to measure your overall perceptions of using multi-method forms of authentication for security while conducting e-commerce activities in public access environments. Your participation in this survey is voluntary and completely anonymous. Responding and submitting your responses to the survey questions indicates voluntary participation in the study.

The survey should take between 15 to 25 minutes to complete. All responses will be kept confidential. Your survey response is vital to the improvement of reducing identity theft and protecting your personal identifying information by reducing invasion of your privacy through a more efficient means of authenticating your access methods. Thank you for your interest and participation in this survey.

Sincerely,
Joseph Marnell, Ph.D. Candidate
Nova Southeastern University
Graduate School of Computer & Information Sciences

Section A. Perceived Value of Organizational Protection (PVOP) of Personal Identifying Information (PII)

Please rate the level of importance you feel about the following statements from (1) Not Important to (7) Extremely Important in regards to having the university protecting your **Personal Identifying Information (PII)**

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP1: Preventing unauthorized access to your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP2: Prevent theft of your PII	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP3: Prevent the use of your PII without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP4: Prevent the collection of your PII during online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP5: Prevent the interception of your online transactions with the school	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP6: Prevent the ability of university personnel to manipulate or change your PII on the university information systems without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP7: Prevent the ability of university personnel to preserve your online transaction PII for their personal interest without your consent	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Item	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP8: Prevent Internet hackers from having access into your PII on the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP9: Prevent Internet hackers from theft of your PII from the university's information system	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)
PVOP10: Prevent Internet hackers from having the ability to intercept, hide, or manipulate some part of your PII from the university's information systems	Not Important (1)	Low Importance (2)	Slightly Important (3)	Neutral (4)	Modestly Important (5)	Very Important (6)	Highly Important (7)

Section B. Invasion of Privacy (IOP)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university protect you from ***Invasion of Privacy (IOP)***

Items	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP1: Protecting my personal data isn't my responsibility	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP2: I will not use university systems for registration because of privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP3: Securing my privacy impedes use of my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP4: I don't have time to deal with privacy issues	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
IOP5: I don't know how to secure my information on my computer	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
IOP6: I don't understand the privacy threats	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section C. Authentication Complexity (AC)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to having the university provide ***multi-method authentication systems (MMAS)*** with minimal ***Authentication Complexity (AC)***

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
AC1: MMAS is more complex to use than previous forms of password identification	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC2: MMAS requires too much time for log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC:3 There are too many MMAS devices required to use	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC4: MMAS would require me to carry additional identification with me at all times to log-in	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC5: MMAS are not accurate enough	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
AC6: MMAS is more complex than just facial recognition	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section D. Resistance to using multi-method authentication system (RMS)

Please rate the level of importance you feel about the following statements from (1) Strongly Disagree to (7) Strongly Agree in regards to your resistance to using *multi-method authentication systems (MMAS)* for university identification

Items	Strongly Disagree	Disagree	Somewhat Disagree	Neither Disagree nor Agree	Somewhat Agree	Agree	Strongly Agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
RMS1: I am opposed due to MMAS requiring skill changes	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS2: I am opposed to using any MMAS	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS3: I prefer my previous authentication methods as it is easier	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS4: I am opposed to MMAS to protect my PII	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS5: I am opposed to using MMAS due to process uncertainty	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS6: I am opposed to using MMAS due to privacy concerns	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)
RMS7: My opposition to MMAS will influence my attendance of the university	Strongly Disagree (1)	Disagree (2)	Somewhat Disagree (3)	Neither Disagree nor Agree (4)	Somewhat Agree (5)	Agree (6)	Strongly Agree (7)

Section E. Demographic information.

Gender: Male Female
Age: 18 or under 19-24 25-29 30-34
 35-39 40-54 55-59 60 or older

Degree Major Education Business Arts Science
 Religion Mathematics Other

Academic Level Freshman Sophomore Junior Senior
 Bachelors Masters Other

How man incidents of any form of privacy intrusion or identity theft have you experienced?
 0 1 2-3 4-5 6 or more

How man incidents of any form of privacy intrusion or identity theft has anyone in your family,
at work, school, or an acquaintance experienced?
 0 1 2-3 4-5 6 or more


Appendix E

Expert Review Questionnaire

Thanks for participating in this review. Please provide your anonymous feedback regarding the research instrument attached. If required, please use additional paper.

1. Are the directions for completing the instrument clear and complete? YES NO

If no, please explain



2. Do the items appropriately measure the construct being evaluated? YES NO

If no, please explain



3. Are there any items that you would recommend revising? YES NO

If yes, please explain



4. Would you recommend deleting any items? YES NO

If yes, please explain



5. Would you recommend including any additional items in this instrument? YES NO

If yes, please explain



Appendix F

E-Mail to Expert Panel

Dear Information Security Expert,

My name is Joseph Marnell and I am a Ph.D. candidate at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled “An Empirical Investigation of Factors Affecting Resistance to Using Multi-method authentication systems in Public-Access Environments.” This study will attempt to assess the aspects of the Perceived Value of Organizational Protection of PII (PVOP), authentication complexity (AC), and invasion of privacy (IOP) by individuals in predicting their resistance to using multi-method authentication systems (RMS) in public-access environments to achieve greater user biometric understanding. The information obtained from this study could prove valuable in understanding users’ resistance to using multi-method authentication systems within public access environments.

I am asking you to kindly contribute to this study as a member of an expert panel, by completing an anonymous online questionnaire about the Web-based quantitative survey instrument that was developed for the study participants. The study participants will include students based on their academic level (freshman, sophomore, junior, and senior), primary degree, and an equal percentage of each gender. There will be created a control and experimental group of equal size as best as possible. Your anonymous participation in this survey will be limited to reviewing the Web-based quantitative survey instrument and provide feedback about it.

Attached to this e-mail is a copy of the preliminary quantitative survey instrument. Your assistance is being sought, as an expert, to review the preliminary instrument and perform a

qualitative evaluation of the instruments validity by answering five questions. Your response to these questions will assist in making a determination of whether or not the individual items serve to measure the constructs being evaluated and in the identification of additional items that could enhance the instrument. Additionally, there will be a general comments section where you can provide information on the content and structure of the instrument. Your feedback will be used to adjust the attached instrument as required. Your review and feedback should take approximately 30-45 minutes to complete, however, you may take as much time as you chose. Once completed, please click the “Done” button to submit your completed expert panel feedback. Any information provided will only be used as part of this study.

If you are willing to participate, please click the link below for access.

(The survey URL link was inserted here upon the creation of the survey).

Your completion of the expert panel feedback indicates your voluntary participation. If you have any questions regarding this study, you may contact me at marnellj@wbu.edu.

Thanks for your consideration and I appreciate your assistance.

Regards,

Joseph W. Marnell, Ph.D. Candidate

Appendix G

Follow-up E-Mail to Expert Panel

My name is Joseph Marnell and I am a Ph.D. Candidate student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled “An Empirical Investigation of Factors Affecting Resistance to Using Multi-method authentication systems in Public-Access Environments.” Your assistance is being sought, as an expert, to review the preliminary instrument and perform a qualitative evaluation of the instruments validity by answering five questions. Your response to these questions will assist in making a determination of whether or not the individual items serve to measure the constructs being evaluated and in the identification of additional items that could enhance the instrument. Additionally, there will be a general comments section where you can provide information on the content and structure of the instrument. Your feedback will be used to adjust the attached instrument as required. The survey should take approximately 30-45 minutes to complete; however, you may take as much time as you chose. Once completed, please click the “Done” button to submit the completed survey. Any information provided will only be used as part of this study.

If you are willing to participate, please click the link below for access.

(The survey URL link was inserted here upon the creation of the survey)

However, if you are unable to participate as an expert panel member, please forward an email to marnellj@wbu.edu as soon as possible. This will allow time for a possible replacement member to be requested to participate.

Your completion of the survey indicates your voluntary participation. If you have questions regarding this study, you may contact me at marnellj@wbu.edu.

Thanks for your consideration and I appreciate your assistance.

Regards,

Joseph W. Marnell

Appendix H

E-Mail to Main Population

Dear Students,

My name is Joseph Marnell and I am a Ph.D. candidate at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled “An Empirical Investigation of Factors Affecting Resistance to Using Multi-method authentication systems in Public-Access Environments.”

I am inviting you to participate in this study as a member of our university, by completing an anonymous online survey. Participation in this survey is voluntary, at your discretion, and completely anonymous to protect your personal identifiable information and privacy.

The survey will be comprised of 32 questions. There will be a training period provided as part of the survey. The questions should take no more than 15-20 minutes to complete; however, you may take as much time as you chose. Once completed, please click the “Done” button to submit the completed survey. Any information provided will only be used as part of my research and no personally identifiable information is being collected.

If you are willing to participate, please click the link below for access.

(The survey URL link will be inserted here upon the creation of the survey)

Your completion of the survey indicates your voluntary participation. If you have questions regarding this study, you may contact me at marnellj@wbu.edu.

Thanks for your consideration and I appreciate your assistance.

Regards,

Joseph W. Marnell, Ph.D. Candidate

Appendix I

Follow-up E-Mail to Main Population

My name is Joseph Marnell and I am a Ph.D. student at the Graduate School of Computer and Information Sciences, Nova Southeastern University. Currently, I am working on my dissertation research titled “An Empirical Investigation of Factors Affecting Resistance to Using Multi-method authentication systems in Public-Access Environments.”

If you are willing to voluntarily participate, please click the link below for access.

(The survey URL link was inserted here upon the creation of the survey)

Participation in this survey is at your discretion and I will not know who completes this survey.

Your completion of the survey indicates your voluntary participation. If you have questions regarding this study, you may contact me at marnellj@wbu.edu.

This email is being provided to you as a university student as a follow-up request to ask for your voluntary participation in my dissertation research.

If no response is received, a final contact will be offered in class by each faculty member.

Thanks for your consideration and I appreciate your assistance.

Regards,

Joseph W. Marnell

Appendix J
Wayland Baptist University
IRB Approval

Research Review Notification
Issued by the IRB

Researcher(s) involved with proposed study: Joseph Marnell

Date: 08/01/2014

Title of proposal: An Empirical Investigation of Factors Affecting
Resistance to Using Multi-Method Authentication Systems in Public-Access
Environments

Type of Review: Exempt _____ Expedited X Full _____

The decision of the committee is as follows:

- Approved
- Approved with the following recommendations/comments:

- Disapproved
- Comments:

Reviewer(s) Signature(s): _____

Chair, IRB *Joseph Marnell* Date 10/29/2014

Executive Vice President/Provost

_____ Date _____

Appendix K
Nova Southeastern University
IRB Approval



NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Joseph Marnell
From: Ling Wang, Ph.D.
Institutional Review Board

Date: Dec. 5, 2014

Re: *An Empirical Investigation of Factors Effecting Resistance to Use Multi-Authentication Systems in Public-Access Environments*

IRB Approval Number: wang08151405

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE REACTIONS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

References

- Adams, A., & Chang, S. Y. (1993). An investigation of keypad interface security. *Information & Management, 24*(1), 53-59.
- Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.
- Albirini, A. (2006). Teachers' attitudes toward information and communication technologies: The case of the Syrian EFL teachers. *Computers & Education, 47*(4), 373-398.
- Al-Harbi, A., & Osborn, S. (2011). Mixing privacy with role-based access control. *Proceedings of the Fourth International Conference on Computer Science and Software Engineering*. ACM: New York, NY, pp. 1-7.
- Alison, P. A. (1998). *Multiple regression: A primer*. Thousand Oaks, CA: Pine Forge Press/Sage Publications.
- Allison, S., Schuck, A., & Lersch, K. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33*(1), 19-29.
- Altinkemer, K., & Wang, T. (2011). Cost and benefit analysis of authentication systems. *Decision Support Systems, 51*(3), 394-404.
- Altman, I., 1976. Privacy. A concept analysis. *Environment and Behavior, 8*(1), 7-29.
- Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal Economic Perspectives, 22*(2), 171-192.
- Anwar, M., Greer, J., & Brooks, C. (2006). Privacy enhanced personalization in e-learning. *Proceedings of the 2006 International Conference on Privacy, Security and Trust, 380*(1), pp. 42.
- Attaran, M. (2006). The coming age of RFID revolution. *Journal of International Technology and Information Management, 15*(4), 77-88.
- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215.
- Barton, B., Byciuk, S., Harris, C., Schumack, D., & Webster, K. (2005). The emerging cyber risks of biometrics. *Risk Management, 52*(10), 26-31.
- Bauer, I. (1994). *Patients' privacy. Developments in nursing and health care*. Avebury, Aldershot, UK.

- Bellah, J. (2001). Training: Identity theft. *Law and Order*, 49(10), 222-226.
- Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM*, 48(4), 101-106.
- Bhattacharyya, S., JHA, S., Tharakunnel, K., & Westland, J. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3), 602-613.
- Bishop, M., (2005). Psychological acceptability revisited. In: Cranor, L.F., Garfinkel, S. (Eds.), *Security and Usability*. O'Reilly, 1–11 (Chapter 1).
- Blades, M. (2009). Stimulus bill tightens HIPAA privacy requirements. *Security Technology Executive*, 19(6), 36.
- Bolton, R., & Hand, D., (2002). Statistical fraud detection: A review. *Journal of Statistics*, 17(3), 235-255.
- Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, 15(4), 267-293.
- Boudreau, M., Gefen, D., & Straub, D. (2001). Validation in information systems research: A state-of-the-art. *MIS Quarterly*, 25(1). 1-16.
- Brady, J., W. (2010). An investigation of factors that affect HIPAA security compliance in academic medical centers. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (100) http://nsuworks.nova.edu/gscis_etd/100.
- Brown, B. (2009a). New technologies have created new threats to electronic protected health information. *Journal of Health Care Compliance*, 11(4), 35-38.
- Brown, B. (2009b). Privacy provisions of the American recovery and reinvestment act. *Journal of Health Care Compliance*, 11(3), 37-40.
- Burgoon, J., 1982. Privacy and communication. *Communication Yearbook*, 6(1), 206–249.
- Cases, A., Fournier, C., Dubois, P., & Tanner, J. (2010). Web site spill over to email campaigns: the role of privacy, trust, and shoppers' attitudes. *Journal of Business Research*, 63(1), 993-999.
- Cassidy, S., & Eachus, P. (2002). Developing the computer user self-efficacy (CUSE) scale: Investigating the relationship between computer self-efficacy, gender and experience with computers. *Journal of Educational Computing Research*, 26(2), 133-153.
- Cate, F. H. (2006). The failure of fair information practice principles. In Winn, J.K. (Ed.), *Consumer Protection in the Age of the Information Economy*. Ashgate, Aldershot, UK.

- Cazier, J. A., Wilson, E. V., & Medlin, B. D. (2007). The role of privacy risk in IT acceptance: An empirical study. *International Journal of Information Security and Privacy*, 1(2), 61-73.
- Center for Democracy and Technology (2000), Fair information practices. Retrieved August 2008 from: www.cdt.org/privacy/guide/basic/fips.html.
- Chandra, A., & Calderon, T. (2005). Challenges and constraints to the diffusion of biometrics in information technology. *Communications of the ACM*, 48(12), 101-106.
- Chen, C. K., & Hughes, J. (2004). Using ordinal regression model to analyze student satisfaction questionnaires. *Association for Institutional Research*, 1, 1-21.
- Cicchetti, D. V., Showalter, D., & Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation. *Applied Psychological Measurement*, 9(1), 31-36.
- Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones—A survey of attitudes and practices. *Computers and Security*, 24(7), 519-529.
- Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *Computers and Security*, 26(1), 109-119.
- Clodfelter, C. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17(3), 181-188.
- Collins, J. M. (2003). Business identity theft: The latest twist. *Journal of Forensic Accounting*, 1, 303-306.
- Compeau, D., & Higgins, C. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2), 189-211.
- Connell, N. A. D., & Young, T. P. (2007). Evaluating healthcare information systems through an enterprise perspective. *Information & Management*, 44(4), 433-40.
- Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design & analysis issues for field settings*. Chicago: Rand McNally.
- Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. *ACM*, 5, 153-160.
- Cronbach, L. J. (1951). Coefficient Alpha and the internal consistency of test. *Psychometrika*, 16(1), 297-334.
- Creswell, J. W., (2003). *Research design: Qualitative, quantitative, and mixed-methods approach* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Danchev, D. (2011). Google intros advanced sign-in feature. *ZDNet*, 10.

- D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, 89, 59-71.
- DataLossDB. (2010). *Incidents*. Retrieved May 15, 2010, from [http://datalossdb.org/search?direction=desc&order=reported_date&org_type\[\]=Med](http://datalossdb.org/search?direction=desc&order=reported_date&org_type[]=Med).
- Davis, D. F., Bagozzi, P. R., & Warshaw, R. P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.
- DeLone, W., & McLean, E. (2003). Information systems success: The quest for the dependent variable. *Information Systems research*, 3(1), 60-95.
- DeLone, W., & McLean, E. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), 9-30.
- De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D., & Fischer, M. (2002). VIP: a visual approach to user authentication. *Proceedings of the Working Conference on Advanced Visual Interfaces AVI*, ACM Press, pp. 316-323.
- Dhamija, R., & Perrig, A. (2000). A user study using images for authentication. *Proceedings of 9th USENIX Security Symposium*, 9, pp. 4-4.
- Doolin, B., Dillon, S., Thompson, F., & Corner, J. (2005). Perceived risk, the Internet shopping experience and online purchasing behavior: A New Zealand perspective. *Journal of Global Information Management*, 13(2), 66-88.
- Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research*, 21, 119-134.
- Dykes, M. (2016). Buying and selling via head and hand scanning on verge of becoming mainstream. Retrieved April 09, 2016 from <http://skywatchtv.com/2016/04/05/buying-selling-via-head-hand-scanning-verge-becoming-mainstream/>
- Eisenstein, E. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, 61(11), 1160-1172.
- Ellis, T. J., & Levy, Y. (2008). Framework of problem-based research: *A guide for novice researchers on the development of a research-worthy problem*. *Informing Science: the international Journal of an Emerging Transdiscipline*, 11(1), 17-33.
- Federal Trade Commission (FTC). (2008). *Consumer fraud and identity theft complaint data*. Washington, DC: Consumer Sentinel and the Identity Theft Data Clearinghouse.
- Fichtman, P. (2001). Preventing credit card fraud and identity theft: A primer for online merchants. *Information Systems Security*, 10(5), 1-8.

- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.
- Flaherty D. (1967). *Privacy in colonial New England*. Charlottesville: University of Virginia Press.
- Fogel, J., & Nehmad, E. (2009). Internet social networking communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160.
- FTD (1998). *Privacy online: a report to congress*. Federal Trade Commission, available at: www.ftc.gov/reports/privacy3/priv-23a.pdf (accessed 13 August 2008).
- Furnell, S. (2005). Why users cannot use security. *Computers & Security*, 24(4), 274- 279.
- Furnell, S. (2007a). A comparison of Website user authentication mechanisms. *Computer Fraud and Security*, 2007(9), 5-9.
- Furnell, S. (2007b). Making security usable: Are things improving? *Computers and Security*, 26(1), 434-443.
- Furnell, S. (2007c). Identity impairment: The problems facing victims of identity fraud. *Computer Fraud and Security*, 2007(12), 6-11.
- Furnell, S. (2008). End-user security culture a lesson that will never be learnt? *Computer Fraud and Security*, 2008(4), 6-9.
- Furnell, S. (2010). Jumping security hurdles. *Computer Fraud and Security*, 1(6), 10-20.
- Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers and Security*, 26(5), 410-417.
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computer & Security*, 31(1), 983-988.
- Furnell, S., Dowland, P., Illingworth, H., & Reynolds, P. (2000). Authentication and supervision: A survey of user attitudes. *Computers & Security*, 19(6), 529-539.
- Furnell, S., Papadopoulos, I., & Dowland, P. (2004). A long-term trial of alternative user authentication technologies. *Information Management and Computer Security*, 12(2), 178-190.
- Furnell, S., & Thomson, K. (2009). From culture to disobedience: recognizing the varying user acceptance of IT security. *Computer Fraud & Security*, 5-10.
- Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, 27(7-8), 235-240.

- Gay, L. (1996). *Educational research: Competencies for analysis and application (4th ed.)*. New York, NY: Macmillan.
- Gefen, D., Straub, D. W., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4(7)*, 1-77.
- Gefen, D., & Pavlou, P. A. (2012). The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research, 23(3-Part-2)*, 940-959.
- Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime, 17(4)*, 441-458.
- Gritzalis, S. (2004). Enhancing Web privacy and anonymity in the digital era. *Information Management and Computer Security, 12(3)*, 255-288.
- Gunson, N., Marshall, D., McInnes, F., & Jack, M. (2011). Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits. *Interacting with Computers, 23(4)*, 57-69.
- Gunson, N., Marshall, D., Morton, H., & Jack, M. (2010). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security, 30(4)*, 208-220.
- Gurwitz, P. M. (1987). Ipsative rescaling: An answer to the response set problem in segmentation analysis. *Journal of Advertising Research, 27(3)*, 37-43.
- Hair, J. F., Anderson, R. E., Tatham, R. L. & Black, W. C. (1984). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.
- Hart, D. (2008). Attitudes and practices of students towards password security. *Journal of Computing Sciences in Colleges, 23(5)*, 169-174.
- Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security, 4(4)*, 3-20.
- Heinssen, R., Glass, C., & Knight, L. (1987). Assessing computer anxiety: Development and validation of the computer anxiety rating scale. *Computers in Human Behavior, 3(1)*, 49-59.
- Helms, M. M., Moore, R., & Ahmadi, M. (2008). Information technology (IT) and the healthcare industry: A SWOT analysis. *International Journal of Healthcare Information Systems and Informatics, 3(1)*, 75-92.
- Hertel, B. R. (1976). Minimizing error variance introduced by missing data routines in survey analysis. *Sociological Methods Research, 4(4)*, 459-474.

- Higgins, G., Hughes, T., Ricketts, M., & Wolfe, S. (2008). Identity theft complaints: Exploring the state-level correlates. *Journal of Financial Crime*, 15(3), 295-307.
- Hiltgen, A., Kramp, T., & Weigold, T. (2006). Secure Internet banking authentication. *IEEE Security and Privacy*, 4(2), 21-90.
- Hinde, S. (2005). Identity theft and fraud. *Computer Fraud and Security*, 6, 18-20.
- Hodge, V. J., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review*, 22(2), 85-126.
- Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society*, 31(1), 406-413.
- Hourihan, C. (2009, May 25). *Recap: A CMS & NIST HIPAA Security Rule conference*. Message posted to <https://www.hitrustcentral.net/blogs/ht/archive/2009/05/25/recap-a-cms-amp-nist-HIPAA-security-rule-conference.aspx>.
- Huxian, L., & Liaojun, P. (2009). A novel biometric-based authentication scheme with privacy protection. *Information Assurance and Security*, 2, 295-298.
- Identity Theft Resource Center. (2012). 2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier. Retrieved February 26, 2012, from http://www.IDTheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2011_20120207.pdf.
- Igbaria, M., & Iivari, J. (1998). Microcomputer utilization patterns among managers and professionals: The case in Finland. *Journal of Computer Information Systems*, 38(3), 28-43.
- Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 91-98.
- Jain, A. K., & Ross, A. (2004). Multibiometric systems. *Communications of the ACM*, 47(1), 34-40.
- Javelin Strategy and Research (2012). Survey: ID theft on the rise again, card victims jump by 2 million annually. Retrieved February 26, 2012, from <https://www.javelinstrategy.com/news/1314/92/Identity-Fraud-Rose-13-Percent-in-2011/d.pressRoomDetail>.
- Jerman-Blažič, B., & Klobucar, T. (2005). Privacy provision in e-learning standardized systems: Status and improvements. *Computer Standards and Interfaces*, 27(6), 561-578.
- Jiang, J., Waleed, J., Muhanna, A. & Klein, G. (2000). User resistance and strategies for promoting acceptance across system types. *Information & Management*, 37(1), 25-36.

- Johnston, J., Eloff, JHP, Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, 22(8), 675-84.
- Jones, M. (1991). Privacy: A significant marketing issue for the 1990s. *Journal of Public Policy and Marketing*, 10(1), 133-148.
- Joppe, M. (2000). *The research process*. Retrieved February 15, 2013, from <http://www.ryerson.ca/~mjoppe/rp.htm>.
- Karyda, M., Gritzalis, S., Park, J., & Kokolakis, S. (2009). Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. *Internet Research*, 19(2), 194-208.
- Kim, M., & Ahn, J. (2007). Management of in the e-marketplace: The role of the buyer's experience in building trust. *Journal of Information Technology*, 23(2), 119-132.
- Kim, W., Jeong, O., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 36(3), 675-705.
- Kirk, J., & Miller, M. L. (1986). *Reliability and validity in qualitative research*, Beverly Hills, CA: Sage Publications.
- Klaus, T., Wingreen, S., & Blanton, E. J. (2010). Resistant groups in enterprise system implementations: A Q-methodology examination. *Journal of Information Technology*, 25(1), 91-106.
- Komarek, R. P., & Moore, W. A. (2004). Fast robust logistic regression for large sparse datasets with binary outputs. *British Ecological Society Journal of Ecology*, 92, 372-383.
- Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 46(1), 254-264.
- Lacoehe, H., Crane, S., & Phippen, A. (2006). Trustguide. Available from: <http://www.trustguide.org>.
- Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52(2), 353-363.
- Laudon, K., & Laudon, J. (2010). *Management information systems: Managing the digital firm* (11th ed.). London, UK: Pearson Education.
- Leedy, D. P., & Ormrod, E. J. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Leidner, D. E., & Jarvenpaa, S. L. (1995). The use of information technology to enhance management school education: A theoretical view. *MIS Quarterly*, 19(3), 265-291.

- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.
- Levy, Y. (2007). Comparing dropouts and persistence in e-learning courses. *Computers & Education*, 48(2), 184-204.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, 51(4), 1664-1675.
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline*, 9, 181-212.
- Levy, Y., & Murphy, K. E. (2002). Toward a value framework for online learning systems. *Proceeding of the 35th Hawaii International Conference on System Sciences*, Big Island, Hawaii, pp. 5-14.
- Levy, Y., & Ramim, M. M. (2009). Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). *Interdisciplinary Journal of E-Learning and Learning Objects*, 1(5), 379-397.
- Levy, Y., & Ramim, M. M. (2010). Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus Wide Information Systems*, 28(1), 102-113.
- Lewis, J. R. (1993). Multipoint scales: Mean and median differences and observed significance levels. *International Journal of Human-Computer Interaction*, 5(4), 383-392.
- Lewis, R. B., Templeton, F. G., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems*, 14, 388-400.
- Lin, H. (2007). Knowledge sharing and firm innovation capability: An empirical study. *International Journal of Manpower*, 28(3/4), 315-332.
- Litwin, M. S. (1995). *How to measure survey reliability and validity*. London, UK: Sage Publications.
- Mattord, H. J., Levy, Y., & Furnell, S. (2012). Assessing relative weights of authentication components: An expert panel approach. *Proceedings of the Seventh Pre-ICIS Workshop on Information Security and Privacy, Orlando*, pp. 1-16.
- Mayer, R., Davis, J., & Schoorman, D. (1995). An integrative model of organizational trust. *Academic of Management Review*, 20(3), 709-734.
- McDaniel, G. (1994). *IBM dictionary of computing*. New York, NY: McGraw-Hill.

- Mertler, C., & Vanatta, R. (2001). *Advanced and multivariate statistical methods: Practical application and interpretation*. Los Angeles, CA: Pyrczak.
- Miller, G.A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, *63*, 81-97.
- Miller, W. R., & Rollnick, S. (2002). *Motivational interviewing: Preparing people for change (2nd ed.)*. New York, NY: Guilford Press.
- Millett, L., & Holden, S. (2003). Authentication and its privacy effects. *IEEE Internet Computing*, *7*(6), 54-58.
- Miltgen, C., Popac, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the “big 3” of technology acceptance with privacy context. *Decision Support Systems*, *56*(1), 109-114.
- Mordkoff, J. T. (2011). *Assumptions of normality*. Retrieved online: February 10, 2016.
- Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192-222.
- Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). Chip and PIN is broken. *Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP)*, pp. 433-446.
- Myers, M., & Avison, D. (2002). *Qualitative research in information systems*. Thousand Oaks, CA: Sage Publications.
- Nandakumar, K. (2008). Multibiometric systems: Fusion strategies and template security. Unpublished doctoral dissertation, Michigan State University: Lansing, MI.
- Neuman, W. L. (1997). *Social research methods – qualitative and quantitative approaches (3rd ed.)*. Boston, MA: Allyn and Bacon.
- Newman, G. R. (2004). Identity theft, problem-oriented guides for police (problem-specific guides series, No. 25), Washington, DC: U.S. Department of Justice.
- Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior*, *26*(3), 406-418.
- O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality and Quantity*, *41*, 673-690.
- O'Brien, J. (2002). *Management information systems: Managing information technology in the e-business enterprise*. Boston, MA: McGraw Hill.

- O’Gorman, L. (2003). Comparing passwords, tokens and biometrics for authentication. *Proceedings of the IEEE*, 91(12).
- Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, 42(1), 15-29.
- Paine, C., Reips, U., Steiger, S., Joinson, A., & Buchanan, T. (2007). Internet users’ perceptions of privacy concerns’ and privacy actions. *International Journal of Human-Computer Studies*, 65(1), 526-536.
- Palmer, A. (2008). Criteria to evaluate automated personal identification mechanisms. *Computers & Security*, 27(7-8), 260-284.
- Palmer, A. (2010). Approach for selecting the most suitable automated personal identification mechanism (ASMSA). *Computers & Security*, 29(7), 785-806.
- Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management and Computer Security*, 18(2), 124-139.
- Penny, K. I. (1996). Appropriate critical values when testing for a single multivariate outlier by using the Mahalanobis distance. *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, 45(1), 73-81.
- Perez, J. F. (2013). An Investigation of Run-time Operations in a Heterogeneous Desktop Grid Environment: The Texas Tech University Desktop Grid Case Study. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (273) http://nsuworks.nova.edu/gscis_etd/273.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing*, 19(1), 27-28.
- Phippen, A., & Furnell, S. (2007). Taking responsibility for online protection-why citizens have their part to play. *Computer Fraud & Security*, 8-13.
- Pons, A.P., Polak, P. (2008). Understanding user perspectives on biometric technology, *Communications of the ACM*, 51(9), 115–118.
- Privacy Rights Clearinghouse. (2010). *A chronology of data breaches*. Retrieved May 15, 2010, from <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>.
- Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber-attacks and novice IT management in a small university. *Journal of Cases on Information Technology*, 8(4), 24-34.
- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7-8), 241-253.

- Robey, D., Ross, J., & Boudreau, M. (2002). Learning to implement enterprise systems: An exploratory study of the dialectics of change. *Journal of Management Information Systems*, 19(1), 17-46.
- Ross, A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of Multibiometrics*. London, UK: Springer.
- Roussos, G., & Moussouri, T. (2004). Consumer perceptions of privacy, security, and trust in ubiquitous commerce. *Personal Ubiquitous Computing*, 8(6), 416-429.
- Ruzic, K. (2009). The next evolution of HIPAA security. *Journal of Health Care Compliance*, 11(3), 23-28.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human-computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122-31.
- Schafer, J. L., & Olsen, M. K. (1998). Multiple imputation for multivariate missing-data Problems: A data analyst's perspective. *Multivariate Behavioral Research*, 33(4), 545-571.
- Schuster, E. (1976a). Privacy and the hospitalization experience. *Communicating Nursing Research* 7(1), 153-171.
- Schuster, E. (1976b). Privacy, the patient and hospitalization. *Social Science and Medicine* 10(1), 245-248.
- Sekaran, U. (2003). *Research methods for business – a skill-building approach*. Hoboken, NJ: John Wiley & Sons.
- Shadish, W., Cook, T., & Campbell, D. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston: Houghton Mifflin Company.
- Shareef, M. A., & Kumar, Vinod (2012). Prevent/control identity theft: Impact on trust and consumers' purchase intention in B2C EC. *Information Resources Management Journal (IRMJ)*, 25(3), 30-60.
- Shaw, R. S., Chen, C. C. Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100.
- Shevade, K. S., & Keerthi, S. S. (2003). A simple and efficient algorithm for gene selection using sparse logistic regression. *Oxford University Press*, 19(17), 2246-2253.
- Silicon.com (2005). Banks must boost security to drive online banking. Forrester Research New Article, www.silicon.com [last accessed September 2010].

- Sinclair, S., & Smith, S. (2005). The TIPPI point: Towards trustworthy interfaces. *IEEE Security and Privacy*, 3(4), 68-71.
- Slippery Rock University (2007). Slippery rock adds RFID to student cell phones. Retrieved from <http://www.rfidjournal.com/articles/view?3463>.
- Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information systems security. *Information Systems Management*, 23(2), 23-32.
- Sprinthall, R. (1997). *Basic statistical analysis*. Boston, MA: Allyn and Bacon.
- SPSS® Software (2013). SPSS. [Computer Software]. <http://spss.com>.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 2(13), 147-169.
- Sun, H., & Zhang, P. (2006). The role of moderating factors in user technology acceptance. *International Journal of Human-Computer Studies*, 64(2), 53-78.
- Symantec (2013). Internet security threat report 2013. Retrieved January 31, 2014, from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2(1), 53-55.
- Thompson, R., Compeau, D., & Higgins, C. (2006). Intentions to use information technologies: An integrative model. *Journal of Organizational and End-User Computing*, 18(3), 25-47.
- Tabachnick, B., & Fidell, L. (2001). *Using multivariate analysis*. New York, NY: Harper Collins College Publishers.
- Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics*. Boston: Allyn and Bacon.
- The Yomiuri Shimbun (2016). Fingerprints to be tested as "currency." Retrieved May 15, 2010, from <http://the-japan-news.com/news/article/0002859676>
- Thomas, G., & Botha, R. A. (2007). Secure mobile device use in healthcare guidance from HIPAA and ISO17799. *Information Systems Management*, 24(4), 333-342.
- Trochim, W., & Donnelly, J. (2008). *The research methods knowledge base*. Mason, OH: Cengage Learning.
- Tsalakanidou, F., Malassiotis, S., & Strintzis, M. G. (2007). A 3D face and hand biometric system for robust user-friendly authentication. *Pattern Recognition Letter*, 28(16), 2238-2249.

- Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, 17(5), 207-227.
- Udo, G. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management and Computer Security*, 9(4), 165-174.
- Uzoka, F., & Ndzinge, T. (2009). Empirical analysis of biometric technology adoption and acceptance in Botswana. *The Journal of Systems and Software*, 82, 1550-1564.
- Vagias, W. M. (2006). Likert-type scale response anchors. *Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management*. Clemson University.
- Van Hoose, S. J. (2008). *Attitudes toward biometric authentication/identification for use in student assessment in online courses in higher education*. (Doctoral Dissertation). Retrieved from ProQuest Dissertations and Theses. (Accession Order No. [103008]).
- Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, 24(1), 115-139.
- Venkatesh, V., Morris, M., Davis, F., & Davis, G. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.
- Verplanken, B., & Aarts, H. (2006). Beyond frequency: Habit as mental construct. *British Journal of Social Psychology*, 45(3), 639-656.
- Verplanken, B., & Melkevik, O. (2008). Predicting habit: The case of physical exercise. *Psychology of Sports and Exercise*, 9(1), 15-26.
- Verplanken, B., Myrbakk, V., & Rudi, E. (2005). The measurement of habit. In Betsch, T., & Haberstroh, S: *The Routines of Decision Making*. Laurence Erlbaum: Mahwah, NJ, 2005, 231-247.
- Verplanken, B., & Orbell, S. (2003). Reflections of past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, 33(6), 1313-1330.
- Wang, P., & Petrison, L. (1993). Direct marketing activities and personal privacy: A consumer survey. *Journal of Direct Marketing*, 7(1), 7-19.
- Weir, C., Douglas, G., Carruthers, M., & Jack, M. (2011). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1), 47-62.

Wendels, T., Mählmann, T., & Versen, T. (2009). Determinants of banks risk exposure to new account fraud—Evidence from Germany. *Journal of Banking and Finance*, 33(2), 347-357.

Westin A. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Yan, J., Blackwell, A., Anderson, R. & Grant, A. (2001). The memorability and security of passwords –Some empirical results. *Technical Report No. 500 2001, computer Laboratory University of Cambridge*, <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf>.

Young, J. B. (1978). *Privacy*. Chichester, UK: Wiley & Sons.

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on Internet users' information privacy concerns. *Proceedings of the Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT)*, Port Elizabeth, ZA: 226, pp. 197-204.

Zviran, M., & Erlich, Z. (2006). Identification and authentication: Technology and implementation issues. *Communications of the Association for Information Systems*, 17(4), 90-105.