

Assessing the Use and Acceptance of Combined Biometric and Smart Card Technologies
in Current Forms of Identification in the United States

Dissertation Manuscript

Submitted to Northcentral University

School of Business and Technology Management

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

SILVIA TOVAR-RIVERA

San Diego, California

January 2019

ProQuest Number: 13805385

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 13805385

Published by ProQuest LLC (2019). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

Approval Page

Assessing the Use and Acceptance of Combined Biometric and Smart Card Technologies
in Current Forms of Identification in the United States

By

SILVIA TOVAR-RIVERA

Approved by the Doctoral Committee:

<div>DocuSigned by: <i>Garrett Smiley</i> 458DFCD81B5A4C7...</div>	Ph.D.	02/05/2019 16:34:31 MST
Dissertation Chair: Garrett Smiley	Degree Held	Date
<div>DocuSigned by: <i>Abigail Scheg</i> 792AC842049B4AF...</div>	PhD, MBA	02/06/2019 04:51:00 PST
Committee Member: Abigail Scheg	Degree Held	Date
<div>DocuSigned by: <i>Marie Bakari</i> 8F10EBB525784DB...</div>	DBA, MBA	02/06/2019 09:29:19 MST
Committee Member: Marie Bakari	Degree Held	Date

Abstract

In the United States, law enforcement agencies and the U.S. public are increasingly concerned with battling identity theft and fraud crimes. One potential preventing approach is the utilization of biometric (BIO) and smart card (SC) technologies in current forms of identification. The extensive technology acceptance literature indicates that a significant component of any technology adoption is user acceptance. Thus, further examination of the factors associated with the acceptability of BIO and SC technologies for combating identity theft and fraud is necessary to determine the U.S. public's approval and willingness to use such a system. This quantitative investigation examined whether the U.S. public's perceptions of performance expectancy (PE), perceived credibility (PC), social influence (SI), facilitating conditions (FC), and attitude (Att) were related to their behavioral intention (BI) to use a combined biometric smart card technology (CBIOSCT) for identification purposes in a voluntary setting. This study also evaluated the extent to which the predictions of PE were mediated by the PC variable. Utilizing an extended unified theory of acceptance and use of technology (UTAUT) model as the research conceptual framework, a sample of 145 randomly selected SurveyMonkey audience members residing in six U.S. cities were surveyed on their views to six variables postulated to explain their BI to use a CBIOSCT. The proposed model was assessed utilizing SEM technique and SPSS AMOS software. The mediating effect of PC on PE was also tested using linear regression. The findings suggest that Att and FC were the only determinants that positively predicted the intention to use CBIOSCT. In addition, while PC was not a significant predictor of BI, in the SEM analysis PC was found as an inter-mediator variable in explaining the changes of PE. Together these constructs explained 73% of the variance in BI to use CBIOSCT. Future research should examine the extent to which people's attitudes toward the adoption of a CBIOSCT is

mediated by the FC factor, as this study found a significant correlation between FC and Att, which was not postulated in the conceptual research framework of the study. Other directions of research may include investigating the moderating effect of design, security solutions, service and maintenance on facilitating conditions and whether the role of these factors outweighs the negative effect of privacy and risk perceptions. Finally, qualitative research could also be conducted to further improve the model and to better understand what influences people's positive and negative perceptions of CBIOSCT in current forms of identification to prevent identity theft and fraud.

Acknowledgements

First, I greatly thank God for giving me the love, guidance, inspiration, and endurance to carry out and finish my doctoral degree. To my beloved parents Mardonio and Martha, my sister Carolina, relatives, and friends, I wish to express my gratitude for your continued support and prayers, your help and words of encouragement have been invaluable to me. I want to also show my deep appreciation to my husband Ervin for his love and immeasurable support throughout this doctoral journey. Special thanks go to my amazing daughter Katherine for her endless love and understanding, and for always cheering me up.

My sincere gratitude to my Committee Chair, Dr. Garrett Smiley for his patience, constructive feedback, continuous guidance, and for always pointing me toward the finish line. I would also like to thank my Committee Subject Matter Expert, Dr. Abigail Scheg and my Committee Academic Reader Dr. Marie Bakari, for their insightful comments and knowledge. To you all, I am forever grateful, without your precious support, completing my doctoral study would not be successful.

Table of Contents

Chapter 1: Introduction	1
Statement of the Problem.....	5
Purpose of the Study	6
Theoretical Framework.....	11
Nature of the Study	14
Research Questions.....	17
Research Hypotheses	18
Significance of the Study	19
Definition of Key Terms.....	20
Summary	21
Chapter 2: Literature Review	23
Theoretical Framework.....	24
Summary	58
Chapter 3: Research Methods	60
Research Methodology and Design	63
Population and Sample	66
Materials/Instrumentation.....	69
Operational Definitions of Variables	73
Study Procedures	79
Data Collection and Analysis	80
Assumptions	82
Limitations.....	84
Delimitations.....	87
Ethical Assurances	89
Summary	90
Chapter 4: Findings.....	92
Validity and Reliability of Data.....	94
Results.....	97
Evaluation of Findings.....	131
Summary	136
Chapter 5: Implications, Recommendations, and Conclusions	139
Implications	147
Recommendations for Practice	155
Recommendations for Future Research	160
References	163
Appendices.....	189
Appendix A: Research Questionnaire.....	190
Appendix B: Site Permission	193

Appendix C: Survey Introductory Letter	194
Appendix D: Informed Consent Form	195
Appendix E: G*power Estimated Sample Size	197
Appendix F: Permission to Use Survey Instruments – Loo et al.	198
Appendix G: Permission to Use Survey Instruments – Dr. Morosan	200
Appendix H: Permission to Use Survey Instruments – Bush et al. (2014).....	202
Appendix I: Models and Theories of Individual Acceptance	204
Appendix J: Frequency Table for Survey Items in the Demographic Information Section	205
Appendix K: Summary of Constructs and Corresponding Survey Items	207
Appendix L: Anti-Correlation Matrix.....	208
Appendix M: Reproduced Correlations and Total Variance	210
Appendix N: Scree Plot of Eigenvalues.....	213
Appendix O: Multicollinearity Diagnostics.....	214
Appendix P: SEM Parsimonious Model Multicollinearity Diagnostics	215
Appendix Q: SEM Parsimonious Model Multicollinearity Diagnostics	216

List of Tables

Table 1. Demographic Characteristics of the Sample.....	101
Table 2. Performance Expectancy Frequency Table	102
Table 3. Statistical Analysis of Performance Expectancy	103
Table 4. Perceived Credibility Frequency Table	105
Table 5. Statistical Analysis of Perceived Credibility	105
Table 6. Social Influence Frequency Table	106
Table 7. Statistical Analysis of Social Influence	107
Table 8. Facilitating Conditions Frequency Table.....	109
Table 9. Statistical Analysis of Facilitating Conditions.....	109
Table 10. Attitude Frequency Table	111
Table 11. Statistical Analysis of Attitude	111
Table 12. DV Behavioral Intention Frequency Table.....	112
Table 13. Statistical Analysis of Behavioral Intention to Use CBIOSCT	113
Table 14. Summary of Statistical Analysis for All Variables.....	114
Table 15. Suitability of Sample Size and Data for Factor Analysis	117
Table 16. EFA and Communalities.....	118
Table 17. Convergent Validity, Composite Reliability, and Cronbach's Reliability	119
Table 18. Factor Correlation Matrix and AVE Scores	119
Table 19. Assessment of Normality.....	121
Table 20. Measurement of Model Reliability and Validity	126
Table 21. Summary of Hypothesis Testing.....	128
Table 22. Test of Performance Expectancy Effects.....	129
Table 23. Test of Social Influence Effects.....	130
Table 24. Test of Facilitating Conditions Effects	130
Table 25. Test of Attitude Effects.....	131
Table 26. Performance Expectancy Mediating Effects by Perceived Credibility	131

List of Figures

Figure 1. The conceptual research framework.....	7
Figure 2. Measurement model: Factor loadings, covariance between the residual errors, latent variable covariances, R-square values, and standardized path estimates.	124
Figure 3. Measurement model: Factor loadings, covariance between the residual errors, latent variable covariances, R-square values, and unstandardized path estimates	125
Figure 4. Research parsimonious model: R-square values, and unstandardized path estimates.	128

Chapter 1: Introduction

In the United States, identity theft and identity fraud are vast and growing problems. Identity theft is the illegal acquisition of someone else's personal identification information, such as passwords, private data, personal identification numbers (PINs), or security tokens (Jamieson et al., 2012). Identity fraud involves an individual using information gathered via identity theft or illicitly attempting to use someone else's personal identification information for the purpose of impersonating the victim to commit or attempt to commit criminal acts or achieve personal financial gain (Jamieson et al., 2012). According to the Identity Theft Resource Center (ITRC, 2017), in 2016, there were 1,093 data breaches in the United States, which represented a significant increase of 40% from the 780 data breaches reported in 2015. These breaches exposed more than 36 million records and included information such as Social Security Numbers (SSNs), health reports, drivers' license numbers, passport numbers, addresses, credit and debit card numbers, and bank statements.

Identity theft and fraud can hurt targeted individuals through lost life savings, damaged credit, denied loans, and other serious consequences, such as being liable for debts that are unknown to victims or being incarcerated for crimes caused by identity thieves (Identity Theft, 2000). To safeguard consumers' personally identifiable information (PII), legislators and Congress have passed bills to tackle issues surrounding identity theft and fraud, including the Identity Theft Penalty Enhancement Act (ITPEA) of 2004, the Gramm-Leach-Bliley Act (GLBA) of 1999, and the REAL Identification (ID) Act of 2005 (U.S. Department of Justice [DOJ], 2010). The ITPEA specified punishments for identity thieves who use someone else's identification information to carry out criminal acts (DOJ, 2010). Under the GLBA privacy act, financial institutions must comply with several requirements, including the mandatory use of

security safeguards to protect consumer data from unauthorized disclosure, access, misuse, loss, or alteration (GLBA, 1999). With the Real ID ACT Enhanced Driver's License (EDL) and Enhanced Identification (EID) Card acts, individuals planning to travel by air or to enter any federal agency, including U.S. military facilities, must have an EDL or EID for identity verification (Real ID Act, 2005; U.S. Department of Homeland Security [DHS], 2016b).

According to the DHS (2015), EDL and EID cards will have "a Radio Frequency Identification (RFID) chip that will signal a secure system to pull up your biographic and biometric data . . . and a Machine Readable Zone (MRZ) or barcode that the federal official can read electronically if RFID isn't available" (para. 4). Federal employees and contractors use similar technology throughout the government, called a Smart Card (SC). For example, all Department of Defense (DoD) employees, contractors, and soldiers are required to use a Common Access Card (CAC) in order to access physical, logical, and network DoD resources (DoD, 2014). This identification (ID) card issued by the federal government to its personnel is capable of verifying and confirming the cardholder's identity; storing information about the user; authenticating, recording, and tracing the user's operations; and verifying ID holder privileges to authorize their physical and logical access to systems and data (Draper, Prenzler, & Ritchie, 2012).

CAC technology provides a more rigorous way to confirm and validate the cardholder's identity, as it is used in conjunction with a personal identification number (PIN), public key infrastructure (PKI) authentication tools, personal identity verification (PIV) certificates, and biometric technology (DoD, 2014). Li, Lu, X. Yang, and Y. Yang (2015) suggested that combined SC and biometric (BIO) technology could provide strong verification and validation of the cardholder's identity. This convergence appears to be a promising way to deter identity theft

and fraud, as SC and BIO technology can provide robust data security, validated and verified access, and sturdy protection against exploitation, alteration, and forgery (Li et al., 2015b).

While promising, in the United States, to date, combined biometric and smart card technology (CBIOSCT) in existing forms of personal identification has not been extended beyond required federal government agencies to the private and commercial sector, all government agencies, or nongovernmental organizations. So far, there is limited research on the factors associated with the U.S. public's willingness to adopt CBIOSCT for identity verification in a voluntary setting.

Businesses and governments around the world do their best to acquire the most modern technology in order to boost organizational efficiency and productivity and enhance the safety and well being of the population. Today, technology is not only considered to be a tool for disseminating knowledge (Franks, Krause, & Lynch, 2017), but also as an instrument to tackle changing threats (Calhoun, 2016). However, a vital prerequisite for technology-based inventions and services attaining their full operational capability is to encourage individuals to adopt and enjoy using the technology. According to Brown, Emami, and Smith (2016), the failure of integration of technologies, such as biometrics, is frequently reliant on people's willingness to adopt and use the technology. Consequently, the comprehension of technology acceptance is crucial, because the demand for biometric technology to deliver reliable and high-performance solutions is rising at a rapid pace in both public and private sectors (Byun & Byun, 2013).

The use of CBIOSCT has vastly expanded around the world. The applications of this technology include identity verification and validation, banking, storage and data management, access control, mobile communications, public transport payment, and security (Sweta, 2015). Smart cards with biometric technology have an embedded microchip that can store and process large amounts of data (Ching-Wei, Yen, & Yu-Bing, 2015). According to Li et al. (2015a), a

combined biometric smart card (CBIOSC) offers a safe and convenient authentication or identification of a person, since CBIOSC is difficult to forge. In countries such as Argentina, Belgium, Brazil, Germany, Portugal, and the United Kingdom, the key driving forces for the inclusion of chips in their national ID cards were national security, fraud and crime protection, prevention of counterfeit identification, and increasing effectiveness of government services for their citizens (Council of the European Union, 2010; Fascendini & Roveri, 2014; Federal Public Service for Information and Communication Technology [FEDICT], 2012; Soares, 2011).

In the United States, numerous bills have been introduced in Congress in the midst of concerns about identity crimes. One bill proposed a social security SC with BIO technology (Social Security Identity Theft Prevention Act, 2008). The Real ID Act (2005) implements CBIOSCT for drivers' licenses and state ID cards to increase homeland security. Another bill would mandate a Medicare SC with BIO identifiers to minimize fraud and enhance protection and privacy (Medicare Common Access Card Act, 2015). The U.S. Government Accountability Office (GAO, 2016) conducted a thorough review of hundreds of healthcare fraud cases and found that smart cards are a pioneering solution to avert fraud.

Although the aforementioned factors may still constitute significant barriers that must be taken into account when deploying CBIOSCT, the proposed technology implemented in existing forms of personal identification in the United States could, in theory, bring important benefits to the public and organizations. Such benefits include providing a more reliable, robust, and safe form of identification to deter identity fraud and identity theft crimes (Brown et al., 2016). In this context, the aim of this investigation is to analyze the factors influencing the U.S. public's intent to adopt CBIOSCT in current forms of identification in order to prevent identity theft and identity fraud.

Statement of the Problem

The problem addressed by this study is the escalation of identity theft and fraud, which has become a major source of concern for people and U.S. law enforcement agencies (Cassim, 2015). The number of people affected by identity theft rose from 13.1 million victims in 2015 to 15.4 million victims in 2016 (Marchini, Miller, & Pascual, 2017). A strategy being adopted in many countries to detect and deter identity theft and fraud is the implementation of a smart national identity card (SNIC) (Identity Systems, 2017; Loo, Yeow, & Yuen, 2013). However, refusal to adopt and use individual authentication technologies is identified as a failure factor in CBIOSC technology implementation (Miltgen, Oliveira, & Popovič, 2013). Thus, further examination of the factors associated with the acceptability of BIO and SC technologies for combating identity theft and fraud is warranted.

Various scholars are confident that a convergence of BIO and SC technologies can effectively authenticate and verify the identity of an individual (Das, Mishra, & Mukhopadhyay, 2014; Li et al., 2015a; Karuppiah & Saravanan, 2014); so far, there is limited research on the factors associated with the adoption of these technologies. Different studies examining the public's acceptance of technology in diverse environments confirm the appropriateness of technology acceptance models to determine user adoption and willingness to use such a system (Dečman, 2015; Hino, 2015; Loo et al., 2013; Miltgen et al., 2013). Without a better understanding of the factors influencing user acceptance of BIO and SC technologies, organizations' strategies to adopt CBIOSC for identity theft prevention would be undetermined. Loo et al.'s (2013) pioneering investigation evaluated Malaysian citizens' acceptance of a SNIC for homeland security and explained that further research is needed that focuses on how users accept a SC technology based on the roles it is created to support.

Purpose of the Study

The purpose of this nonexperimental, correlational, quantitative investigation was to examine the relationship between the independent variables of performance expectancy (PE), perceived credibility (PC), social influence (SI), facilitating conditions (FC), and attitude (Att) on the dependent variable of the U.S. public's behavioral intention (BI) to use CBIOSCT. This study also evaluated the extent to which the predictions of PE were mediated by the PC variable. This investigation adds to the understanding of why individuals adopt technology, so that better systems for devising, constructing, and implementing CBIOSC technology can be developed in a way that will increase the chances of user acceptance. Furthermore, comprehending the factors that influence the U.S. public's acceptance of CBIOSCT in current forms of identification for identity theft and identity fraud prevention could provide insight enabling lawmakers, organizations, financial institutions, and identity management service providers to devise suitable future provisions and policy measures to tackle the challenges that identity theft crimes pose that will be worthwhile, effective, and satisfactory to the public.

To determine the factors that shape the U.S. public's acceptance of CBIOSCT, the investigation framework used Loo et al.'s (2013) extension of Davis, Davis, Morris, & Venkatesh's (2003) unified theory of acceptance and use of technology (UTAUT) model to include PE, PC, SI, and FC as independent variables and expanded the model to include Att as another independent variable (see Figure 1). Research instrument items were adapted from instruments developed by Loo et al. (2013), Bush, Cole, and Kohnke (2014), and Morosan (2016). A study survey format was also adapted from Loo et al.'s (2013) original questionnaire. Both research instrument items and survey were modified to fit the investigation context (see Appendix A).

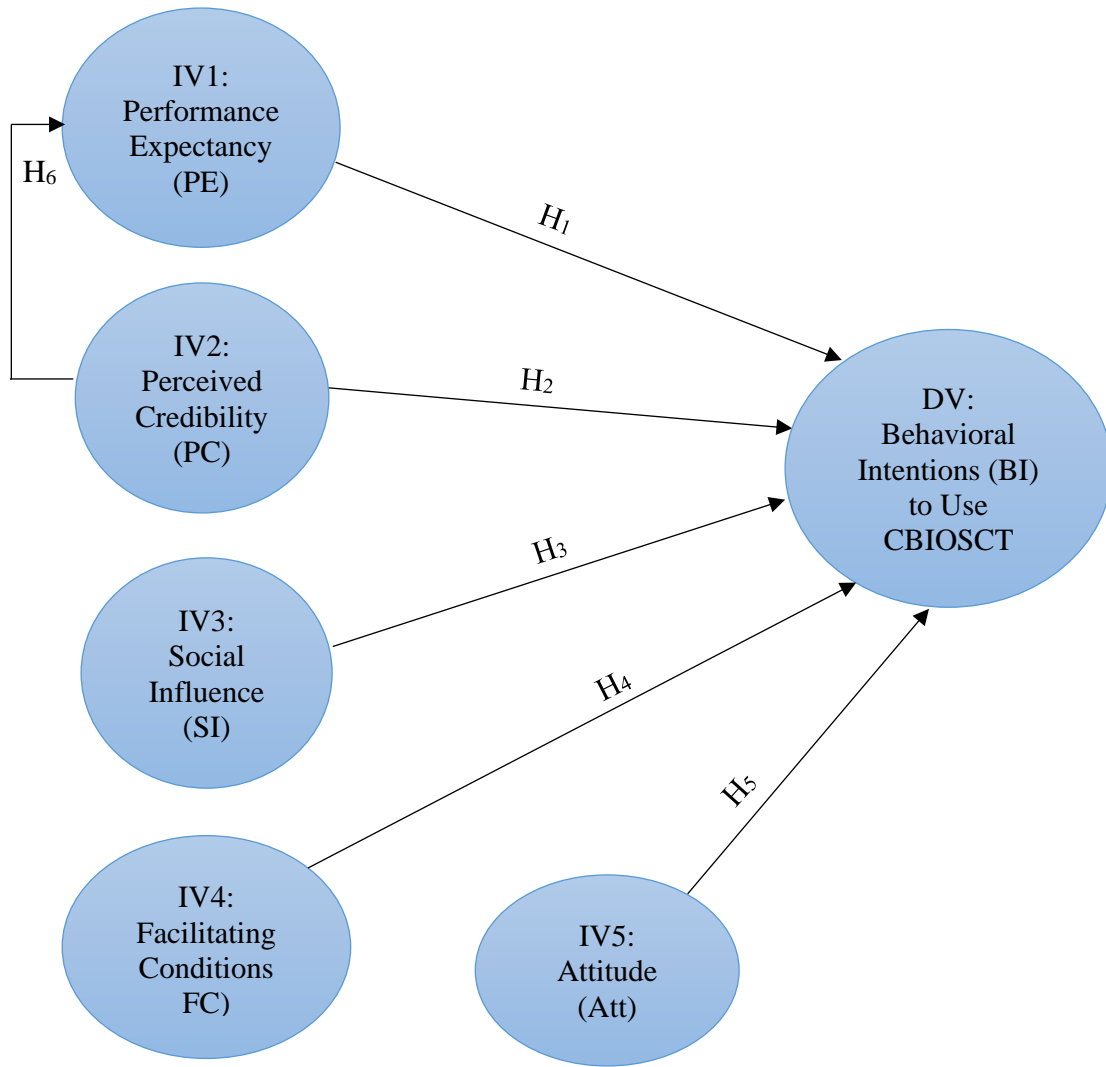


Figure 1. The conceptual research framework.

One hundred online questionnaires were distributed via SurveyMonkey (see Appendix B) among residents 18 years or older of each of the six cities most visited by tourists in the United States—New York, NY; Washington, DC; Orlando, FL; Charleston, SC; Las Vegas, NV; and San Francisco, CA (TripAdvisor, 2016)—for a total of 600 surveys. The site for the research comprised residents of the cities most visited by tourist throughout the United States due to the ease with which safety and security problems could occur. Mansfeld and Pizam (2006) explained

that incidents of security, such as larceny, theft, robbery, rape, murder, piracy, kidnapping, and domestic, international, and cross-border terrorism are more likely to exist in tourist destinations. Due to budget and time constraints, the 600 online surveys were disseminated through SurveyMonkey among randomly selected SurveyMonkey respondents.

Each subject received a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D) with a link to the survey, explaining the purpose of the study and safety measures taken to ensure anonymity. Safety measures include keeping identifying information and survey results anonymous and password protected. In the informed consent form, in the signature section, it was explained that by clicking “Yes”, participants consented to answering the questions in the survey. By answering all questions in the survey, respondents implicitly agreed to participate in the survey. Respondents had the option to withdraw from the survey at any moment; exiting the survey or clicking “No” in the informed consent form signature section denoted that participants did not agree to participate. The questionnaires were distributed only after receiving approval from Northcentral University (NCU)’s Institutional Review Board (IRB).

Structural equation modeling (SEM) and Statistical Package for the Social Sciences (SPSS) Analysis of Moment Structures (AMOS) version 25 software were used to assess the variables under consideration. By using a power of 80%, an alpha significance level of .05, and an effect size of .30, with 1 degree of freedom, the *a priori* power analysis estimated a minimum sample size of 88 (see Appendix E). These elements of power calculations were set based on similar studies that have demonstrated an appropriate use of study (Addo & Attuquayefio, 2014b; Al-Abdallah & Al-Qeisi, 2014; Gaffar, Singh, & Thomas, 2013; Loo et al., 2013).

To determine how the public adopts and uses this technology, variables from the UTAUT model generated additional insights into the investigation of CBIOSCT acceptance. The independent variable performance expectancy assessed how the perceptions of CBIOSCT might enhance cardholders' performance in aiding the government to protect the U.S. public from identity thieves and counterfeiters and enable effective identity authentication. A recent study disclosed that current users with high performance expectancy in the use of ID cards with embedded, integrated circuit chips or smart cards are prone to show a positive attitude towards adopting this technology and their intention to use it (Loo et al., 2013). The independent variable perceived credibility evaluated the extent to which the U.S. public considers whether CBIOSCT will be a secure system in which data is kept confidential, handled securely and effectively, and will be difficult for criminals to forge and modify. Loo et al. (2013) suggested that perceived credibility is associated with the safety of a system, since it is difficult to counterfeit and is not vulnerable to disclosing personal information to wrong parties.

The independent variable social influence explains the extent to which a person is motivated and influenced by others to use new technology (Davis et al. 2003). In this investigation, social influence evaluated whether or not the U.S. public's intention to utilize CBIOSCT is influenced by the views and motivations of someone who holds a meaningful position in their lives. According to Davis et al. (2003), social influence comprises three main determinants: subjective norm, social factors, and image. In addition, it "affects individual behavior through compliance, internalization, and identification" (p. 452).

The independent variable facilitating conditions explained the extent to which the U.S. public considers whether the existence of a specialized, administrative, and technological structure facilitates their acceptance and utilization of CBIOSCT. According to Davis et al.

(2003), the explanation of the facilitating conditions construct encompasses the notions of the following variables: “perceived behavioral control (TPB/Decomposed TPB, Combined TAM and TPB), facilitating conditions (Model of PC Utilization), and compatibility (Innovation Diffusion Theory)” (p. 453). This determinant refers to the circumstances that enable the acceptance of new technology.

Finally, the independent variable Att explained the extent to which the U.S. public favors or disfavors the adoption and use of CBIOSCT. According to Seyal and Turner (2013), attitude refers to a person’s positive or negative responsive behavior to using technology. Davis et al. (2003) suggested that when PE and effort expectancy are excluded from the UTAUT framework, the effect of Att should be considered. In this investigation, the effort expectancy factor was omitted since CBIOSCT is very simple to use: the cardholder shows the ID at the agencies’ request. Thus, Att was incorporated. Since user attitudes toward the use of mobile learning pivot around PE (Hwang, Kim, Lee, & Yoo, 2016), and PE is positively correlated with PC (Loo et al., 2013), in this study, the correlation between PE and Att and between PC and Att were examined, to determine if the same applied to CBIOSCT.

The dependent variable—the U.S. public’s intention to use CBIOSCT—was studied with BI, since CBIOSCT technologies are not readily available to the general public. Previous studies have shown BI to be a reliable and suitable indicator of usage (Addo & Attuquayefio, 2014b; Davis et al., 2003; Loo et al., 2013). In this investigation, the public’s acceptance, as a dependent variable, was assessed using the following elements adapted from Loo et al. (2013): the extent to which participants in the future will adopt and use CBIOSCT for identification purposes (BI1), will predict utilization of CBIOSCT for identity theft and fraud prevention (BI2), and will continue to use CBIOSCT for identity theft and fraud prevention (BI3).

Theoretical Framework

Several researchers have studied various issues that the public takes into account when making a decision to approve or disapprove of novel technologies. Many technology acceptance models and theories have been used in information systems studies to evaluate and measure user acceptance of new systems and their behavioral intention to use them (Addo & Attuquayefio, 2014b; Batane & Motshegwe, 2015; Brown, Chan, Hu, Tam, Thong, & Venkatesh, 2010; Chau, Hu, Sheng, & Tam, 1999; Davis et al., 2003; Gaffar et al., 2013; Loo et al., 2013). Most of these studies have either applied the technology acceptance model (TAM) or UTAUT model to determine which factors motivate users to adopt and use the new system, and all of them have used BI as an adequate prognosticator of new system use (Addo & Attuquayefio, 2014b; Batane & Motshegwe, 2015; Brown et al., 2010; Chau et al., 1999; Davis et al., 2003; Gaffar et al., 2013; Loo et al., 2013).

Most research in the area of BIO and SC technology has been conducted individually (Chong, Loo, & Yeow, 2011; Harby, Kamala, & Qahwaji, 2012; Kamis, Ngugi, & Tremaine, 2011; Morosan, 2012a); there is limited research on the convergence of BIO and SC technology from a public acceptance viewpoint. Du, Lin, and Wen (2015) suggested that BIO and SC technologies used together provide a robust and trustworthy user authentication solution. However, Friedewald and Pohoryles (2013) argued that biometric technology raises privacy concerns. Further, Harinda and Ntagwirumugara (2015) explained that CBIOSCT is vulnerable to “security violations at level of the card, in the supporting communication network, or in the backed system” (p. 98). Even though no biometric technology provides total defense (Das, 2016), research has indicated that the use of smart cards in conjunction with BIO technologies is

more secure against various attacks, verifies users' identity, and prevents theft and fraudulent operations (Gaurav, Ranjan, & Tyagi, 2012; Li et al., 2015b).

Researchers have demonstrated that the UTAUT model is a valuable way to establish the factors that influence individuals to adopt new technologies, such as information and communication technology (ICT) (Addo & Attuquayefio, 2014b), a mobile electronic medical record (Hwang et al., 2016), e-learning technologies (Shaqrah, 2015), biometric technology (Harby et al., 2012), and SC applications (Chong et al., 2011). The eight concepts Davis et al. (2003) studied to formulate UTAUT include: "The theory of reasoned action, the technology acceptance model (TAM), the motivational model, the theory of planned behavior (TPB), a model combining TAM and TPB, the model of PC utilization, the innovation diffusion theory, and the social cognitive theory" (p. 425) (see Appendix I). Davis et al.'s (2003) conceptual framework presented four determinants of individual adoption and usage behavior: "Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), and Facilitating Conditions (FC)" (p. 447). UTAUT has been widely used to comprehend acceptance and use of numerous types of technology in various environments and the usage of this model has shown to have satisfactory reliability and validity (Addo & Attuquayefio, 2014b; Hino, 2015; Loo et al., 2013; Miltgen et al., 2013).

Davis et al. (2003) empirically confirmed UTAUT's legitimacy and soundness. By incorporating the eight concepts mentioned above, the UTAUT prototype offers a better understanding of user technology adoption. Researchers have applied the UTAUT model to examine various questions associated with technology adoption in the tourism industry (Carvajal-Trujillo & Escobar-Rodríguez, 2014), biometric technology in e-shopping (Hino, 2015), healthcare telemedicine equipment (Bush et al., 2014), and the use of a smart national

identity card in Malaysia (Loo et al., 2013). In the UTAUT theoretical structure, Dečman (2015) explained that performance expectancy and social influence are key determinants for explicating individuals' adoption of a specific technology and their intentions to use it.

The literature on UTAUT distinguishes different extensions of this framework and stresses the significance of other factors, such as perceived credibility (Loo et al., 2013), privacy, and experience (Hino, 2015). The UTAUT model applied by Loo et al. (2013) to investigate issues related to Malaysian citizens' approval of SC technology consists of five constructs: performance expectancy, perceived credibility, social influence, facilitating conditions, and anxiety. In this model, performance expectancy and perceived credibility are direct determinants of behavioral intention, and the prediction of the performance expectancy variable is mediated by the perceived credibility variable (Loo et al., 2013). Other scholars have studied the effect of attitude on biometric adoption and propose that this construct is also a predictor of acceptance and intent to use a technology (Seyal & Turner, 2013).

Since the focus of this investigation is on providing a further understanding of the issues surrounding the U.S. public's behavioral intention to adopt CBIOSCT, the UTAUT model was applied. This study used Loo et al.'s (2013) extension of UTAUT and also predicted that PE would be mediated by the PC variable, and expanded the model to include attitude. Even though attitude, which refers to someone's postures of approval or disapproval (Seyal & Turner, 2013), is not an explicit construct in the UTAUT framework, for the purpose of this investigation, attitude was considered to be an essential element in determining the level of approval towards the use of CBIOSCT. The variable of anxiety, proposed by Loo et al. (2013), was not included since stress or nervousness does not arise from using CBIOSCT when the adoption of technology is voluntary. Also, according to Davis et al. (2003), the anxiety factor has an indirect effect on

behavioral intention (BI) through effort expectancy. However, the effort expectancy factor was excluded in this investigation, since using CBIOSCT requires no time or effort, as participants only carry the card and present it to legal entities upon request. Thus, the anxiety factor was judged to be not applicable.

Nature of the Study

The aim of this investigation was to provide a further understanding of the issues surrounding the U.S. public's intention to adopt and use CBIOSCT for identity theft and fraud prevention. Therefore, a nonexperimental, correlational, quantitative approach was used to determine the extent to which the independent variables of PE, PC, SI, FC, and Att were predictive of the dependent variable of the U.S. public's BI to use CBIOSCT, including the extent to which the predictions of PE were mediated by the PC variable. This quantitative approach was the most favorable option since it has been the primary method used in several BIO technology acceptance investigations: Chieh-Heng and Chun-Chieh (2015) used it to evaluate hotel employees' perceptions and adoption of BIO systems; Hino (2015) used it to examine the factors that influence web users' behavioral intent to utilize BIO technology in electronic commerce; and Miltgen et al. (2013) used it to study the factors associated with the acceptability of BIO technologies.

Cano, Sass, and Tumlinson (2014) suggested a nonexperimental, correlational, quantitative approach if the scholar is assessing constructs in their original form with no manipulation, wherein SEM or another method of statistical analysis is used to portray and measure the extent to which two or more constructs are associated when there is no random allocation of subjects to groups. Various scholars (Claydon, 2015; Garza & Landrum, 2015; Park & Park, 2016) have explained that, when the aim of the study is to uncover further

knowledge or develop new theoretical concepts and notions to explain a phenomenon, the choice of a qualitative approach is justified. However, if the aim of the investigation is to test and verify theories and their individual assumptions to generalize to and replicate the results in other subjects and environments, a quantitative method is most suitable (Claydon, 2015; Park & Park, 2016). A nonexperimental, correlational, quantitative approach was most fitting to conduct this investigation, since none of the independent variables (PE, PC, SI, FC, and Att) were manipulated to identify their influence on the dependent variable BI. Moreover, there was no random allocation of subjects to groups, and this study tested the mediation of predictability for the predictor construct of PE by the mediating construct of PC predicting the dependent variable of BI.

The data was gathered using an online survey devised to assess subjects' perspectives and distributed via SurveyMonkey (see Appendix B). The study survey format was adapted from Loo et al.'s (2013) original questionnaire and was administered to randomly selected SurveyMonkey audience members who were residents of New York, NY; Washington, DC; Orlando, FL; Charleston, SC; Las Vegas, NV; and San Francisco, CA. An online survey tool and panel were the best choices, because they are the most robust and prominent tools in scholarly investigations (Balasubramanian, Kasilingam, & Natarajan, 2017; Elbeck, 2014) and they align well with recent studies on technology adoption: Horrey, Lesch, Rahman, and Strawderman (2017) constructed a research questionnaire via SurveyMonkey and administered it to respondents via Amazon Mechanical Turk, to evaluate the predictive relevance of TAM, TPB, and UTAUT to explain motorists' behavioral intent to utilize an Advanced Driver Assistance System (ADAS). Balasubramanian et al. (2017) distributed questionnaires and gathered

responses via SurveyMonkey to examine Asian Indians' intention to use mobile shopping applications.

All scales in the measurement instrument were integrated and slightly modified to fit the U.S. context from validated questionnaires that have been demonstrated to be valid and reliable for assessing users' intentions and acceptance in other environments (Bush et al., 2014; Loo et al., 2013; Morosan, 2016) (see Appendix A). The measurement instrument of this investigation did not put respondents at risk of harm since the confidentiality of respondents remained intact; the online survey was anonymous, with no names, phone numbers, or emails collected.

Questionnaires were distributed only after receiving approval from NCU's IRB. Each construct in this investigation was assessed in the survey instrument by three items, measured using a five-point Likert scale response format ranging from 1 - Strongly Disagree to 5 - Strongly Agree (see Appendix A).

By using a power of 80%, an alpha significance level of .05, and an effect size of .30, with 1 degree of freedom, the *a priori* power analysis estimated a minimum sample size of 88 (see Appendix E). These elements of power calculations were set based on similar studies that have demonstrated an appropriate use of study (Addo & Attuquayefio, 2014b; Al-Abdallah & Al-Qeisi, 2014; Gaffar et al., 2013; Loo et al., 2013). SEM and SPSS AMOS version 25 software were used to assess the variables under research. Furthermore, an exploratory factor analysis (EFA) and a confirmatory factor analysis (CFA) were conducted to examine the underlying relationships in the model, and to assess the fit of the postulated measurement model and causative correlations among independent and dependent variables.

Research Questions

In general, technology acceptance has been a key focus for various researchers due to its importance in comprehending technology dissemination (Bush et al., 2014; Carvajal-Trujillo & Escobar-Rodríguez, 2014). Several scholars have investigated different aspects of technology adoption from diverse theoretical angles, including UTAUT (Addo & Attuquayefio, 2014b; Hino, 2015; Loo et al., 2013; Miltgen et al., 2013). To date, however, despite the compelling attention to comprehending the drivers of technology acceptance, the adoption of CBIOSCT in existing forms of personal identification in the United States for the prevention of identity crimes in a voluntary setting is a relatively new area of research for investigators. Comprehending the forces that shape the public's acceptance of CBIOSCT is crucial for lawmakers, organizations, financial institutions, and identity management service providers to offer an appropriate identity authentication and verification solution, create a perceived high value for citizens, and minimize the cost and incidence of identity crimes.

The following six research questions stemmed from the study purpose and the conceptual framework of the UTAUT model:

RQ1. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT?

RQ2. To what extent, if any, does perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT?

RQ3. To what extent, if any, does social influence predict the U.S. public's behavioral intention to use CBIOSCT?

RQ4. To what extent, if any, do facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT?

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT?

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility?

Research Hypotheses

The six null and six alternative hypotheses that correspond directly to the six research questions are as follows:

H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2₀. Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2_a. Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H6₀. The prediction of performance expectancy is not statistically mediated by perceived credibility.

H6_a. The prediction of performance expectancy is statistically mediated by perceived credibility.

For a visualization of the hypotheses in conjunction with the variables, see Figure 1.

Significance of the Study

The use of CBIOSCT is increasing in both private and public sectors (Walker, 2015). Simultaneously, a lack of comprehension of the challenges and restrictions in implementing current forms of identification with CBIOSCT has resulted in resistance (Kravitz, 2009; Miller & Moore, 1995; Zureik, 2010). In some countries, CBIOSCT identification (ID) cards are seen as a threat to civil rights and an invasion of people's privacy (Laas-Mikko & Sutrop, 2012), while others argue that CBIOSCT ID may enhance security and minimize fraud, due to its ability to verify and authenticate the true identity of a user (Miltgen et al., 2013). Recent investigations about the acceptance of biometric-based technologies have indicated that user perceptions pertain to variables such as perceived usefulness, the efficiency of the system, trust, and the need for security (Hino, 2015; Morosan, 2016). Various scholars and organizations are confident that a convergence of BIO and SC technologies can effectively authenticate and verify the identity of an individual (Das et al., 2014; Karuppiah & Saravanan, 2014; Li et al., 2015a).

To date, however, the adoption of CBIOSCT in existing forms of personal identification for prevention of identity crimes in a voluntary setting is a relatively new area of research for investigators. The results of this investigation could be highly significant and beneficial, especially to governments, private organizations, financial institutions, and identity management service providers. The investigation could provide the aforementioned stakeholders with insight into how to devise suitable future provisions and policy measures to tackle the challenges that identity theft crimes pose that are effective for and satisfactory to the public. Furthermore, comprehending the factors that influence the U.S. public's acceptance of CBIOSCT could potentially accelerate the improvement of current forms of identification, which, in turn, could be a valuable instrument to assist in combating identity theft and fraud in the United States.

Definition of Key Terms

For clarification, important terms used in this investigation are defined below.

Biometric identifiers. Refers to the unique, measurable features employed to characterize and describe people. Some examples include: fingerprints, ear recognition, voice patterns, and palm prints (Rajankar & Shaikh, 2016).

Combined biometric and smart card technology (CBIOSCT). Refers to a standard plastic identification card size embedded with a microchip that can store and process large amounts of data, including biometric identifiers, to provide strong security for user authentication (Jalaliyoon, Sahibuddin, & Taherdoost, 2011).

Drivers. Refers to each independent variable posited to have an impact on the dependent variable (Miltgen et al., 2013).

Identity fraud. Deceit that occurs when an individual uses identity theft or illicitly attempts to use someone else's personal identification information for the purpose of

impersonating the victim to commit or attempts to commit criminal acts for personal financial gain (Jamieson et al., 2012).

Identity theft. The illegal acquisition of someone else's personal identification information, such as passwords, private data, personal identification numbers (PINs), or security tokens (Jamieson et al., 2012).

Intention to use. An individual's willingness to carry out a specific behavior (Ajzen, 1991).

Personally identifiable information (PII). Denotes any data that possesses identifiers exclusive to people, which can be used to identify individuals (Garfinkel, 2015).

Public acceptance. An individual's intentions to use a specific technology for the role it is devised to support (Loo et al., 2013).

Technology acceptance. Denotes a person's desire to utilize a technology for the roles it is created to support (Teo, 2011).

Theory. Implies a systematized and well-thought-out group of interconnected concepts that postulate how variables are related, with the aim of comprehending a phenomenon (Fain, 2004).

Summary

CBIOSCT is customary in numerous nations around the globe, mainly for identity verification and authentication, education, health insurance, electronic payments, public transport, and telecommunications (Ching-Wei et al., 2015). In most countries where CBIOSCT is being used, key driving forces for the inclusion of a chip in the SC have been national security, fraud and crime protection, the prevention of counterfeit identification, and making government services more effective for their citizens (Council of the European Union, 2010; Fascendini &

Roveri, 2014; FEDICT, 2012; Soares, 2011). In fact, various scholars have demonstrated that the implementation of a CBIOSCT can enhance security (Das, Goswami, & Odelu, 2015; Li et al., 2015b) and reduce identity theft (GAO, 2016).

Although in the United States the implementation of CBIOSCT has become a key part of homeland security and government services plans and policies (Medicare Common Access Card Act, 2015; Real ID Act, 2005; Social Security Identity Theft Prevention Act, 2008), there is no academic insight into the degree to which citizens are willing to adopt such technology. Therefore, the aim of this nonexperimental quantitative investigation was to examine the relationship between the independent variables of PE, PC, SI, FC, and Att on the dependent variable of the U.S. public's behavioral intention to use CBIOSCT. The data was gathered by means of an online survey devised to measure participants' behavioral intention to use CBIOSCT. The study population consisted of participants residing in six U.S. cities. Additionally, SEM and SPSS AMOS were used to assess the variables under research.

Comprehending the factors that influence the U.S. public's acceptance of CBIOSCT is crucial for lawmakers, organizations, financial institutions, and identity management service providers to offer an appropriate identity authentication and verification solution, create a high-perceived value for citizens, and minimize the cost and incidence of identity crimes. Furthermore, the results of this investigation will provide the aforementioned stakeholders with insight into how to devise suitable future provisions and policy measures that will be worthwhile, effective, and satisfactory to the public. Finally, understanding the forces that shape the U.S. public's acceptance of CBIOSCT could potentially accelerate the improvement of current forms of identification, which in turn can be valuable instruments in combating identity theft and identity fraud in the United States.

Chapter 2: Literature Review

The purpose of this nonexperimental correlational quantitative investigation is to determine the factors that shape the U.S. public's acceptance of combined biometric and smart card technology (CBIOSCT). This investigation utilized Loo et al.'s (2013) extension of UTAUT to include the independent variables of performance expectancy (PE), perceived credibility (PC), social influence (SI), and facilitating conditions (FC), and expanded the model to include attitude (Att). The effect of each independent variable on the U.S. public's behavioral intentions (BI) to utilize CBIOSCT was examined, and the extent to which the predictions of the variable PE were mediated by the construct of PC was also explored. The data collected could facilitate the comprehension of the factors that influence the U.S. public's acceptance of CBIOSCT in current forms of identification to prevent identity theft and identity fraud.

The literature review starts with a critical analysis of the theoretical framework of the investigation, and the UTAUT model is explored through a comprehensive discussion of its conceptual structure and applications. It continues with a discussion of identification systems, identity theft and identity fraud, smart card-based biometric authentication technology and its applications. Finally, behavioral intentions to adopt and utilize biometric (BIO) and smart card (SC) technologies are inspected from numerous perspectives.

To substantiate the conceptual framework and the modified model of the investigation, a wide assortment of research reports, scholarly and peer-reviewed articles, reference resources, government papers, and books were consulted. These resources were gathered at the Bull Run Regional Library, via Google Scholar, by consulting online newspaper articles, and by utilizing the NCU online library to access databases such as EBSCOhost, Homeland Security Digital Library, IEEE Xplore, ProQuest, SAGE journals, ScienceDirect, and The Springer eJournal. To

search the databases effectively, the following operators were used: AND, full text, scholarly and peer-reviewed journals, and articles published from 2013 forward, although a few resources from previous years were considered. Peer-reviewed journals were the most important sources used in the investigation. The keywords used to search resources efficiently included biometrics AND smart card, biometrics AND UTAUT, biometrics AND technology acceptance, smart cards AND technology acceptance, identity theft victims, identity fraud prevention, and identity verification.

Theoretical Framework

Technology adoption theories. Opposition to and adoption of technologies and determinants of individuals' approval have generated strong interest among researchers. Numerous scholars have elaborated an assortment of contending and complementary concepts, each with a distinctive series of technology acceptance factors. The major concepts and theories of technological adoption that have sought to explain how individuals come to adopt and use a system include the theory of reasoned action (TRA) (Ajzen & Fishbein, 1975), the theory of planned behavior (TPB) (Ajzen, 1991), the technology acceptance model (TAM) (Davis, 1989), the model of personal computer utilization (MPCU) (Higgins, Howell, & Thompson, 1991), the motivational model (MM) (Bagozzi, Davis, & Warshaw, 1992), the diffusion of innovation theory (DIT) (Rogers, 1962), and the unified theory of acceptance and use of technology (UTAUT) (Davis et al., 2003).

In TRA, Ajzen and Fishbein (1975) revealed that a person's acceptance or rejection of a system is shaped by the person's attitude (Att) and subjective norms to carry out the desired conduct. Ajzen and Fishbein (1975) explained that attitudes are composed of the assessment of a belief—that is, the extent to which a behavior is appraised as desirable or undesirable—and the power of the belief, which denotes the strength of a person's convictions. Likewise, subjective

norms are comprised of two elements: “normative belief,” which denotes how a person believes other individuals would like or expect him/her to behave, and “motivation to comply,” which indicates how significant it is for a person to act in accordance with what other people expect (Hoewe & Sherrick, 2015, p. 239).

The TRA model has been applied to various questions associated with behavioral intention in different settings. For instance, Akman, Mishra, and Mishra (2014) employed TRA to explore IT professionals’ desires to undertake green IT and discovered that Att and subjective norms influenced their intention to use and actual utilization. Other scholars have also used TRA to assess attitudes and convictions that may contribute to cyber-bullying among undergraduates and determined that subjective norms predict cyber-bullying perpetration (Doane, Kelley, & Pearson, 2014). Furthermore, Doane et al. (2014) explained that a lack of fellow feeling for undergraduate victims of cyber-bullying, predicts a desirable Att toward cyber-bullying, which in turn, increases the behavioral intent and the cyber-bullying behavior. According to Giumetti, Kowalski, Lattanner, and Schroeder (2014) cyber-bullies often take advantage of online anonymity to impersonate the victim, with the purpose of hiding their real identity. Consequently, the utilization of impersonation as a tactic to communicate online highlights the prevalence of identity theft as a way to effectively target potential victims (Reznik, 2013).

Despite the significant applications of the TRA model, Ahmed, Basoglu, and Daim (2007) acknowledged some drawbacks, such as the danger of conflating Att and subjective norms, because Att can frequently be reexamined as subjective norms, or vice versa. Another drawback is the assumption that conduct assessed using TRA is completely voluntary, but involuntary behaviors and environmental constraints can restrict free will actions. Moreover, Ahmed et al. (2007) indicated that, in an attempt to tackle the weaknesses of TRA and enhance

the predictive strength of TRA, Ajzen (1991) developed TPB, which adds the perceived behavioral control factor to the TRA model as an additional determinant of behavioral intent. Perceived behavioral control concerns the perceived effortlessness or complexity of implementing a particular conduct (Ajzen, 1991). With perceived behavioral control, the general idea is that the perceptions of the existence of control elements, such as knowledge, self-efficacy, and the external environment, enable or impede the public from carrying out the behavior of interest (Choi, Ham, Kim, & Yang, 2013).

Some scholars have argued that the TPB still presents the same TRA limitation, by assuming that a person's behavior is voluntary and based on reason, ignoring involuntary behaviors and unconscious reasons that can restrict free will actions (Bargh, Gollwitzer, & Sheeran, 2013). However, many others have demonstrated that the TPB can explain the association between variables and reveal certain factors that can influence the approval or use of systems (Salim, Sawang, & Sun, 2014; Seyal & Turner, 2013). For instance, a survey investigation of 132 students at a Chinese college revealed that the Att and subjective norms factors impact Chinese undergraduates' intention to adopt e-learning systems (Salim et al., 2014). Likewise, Salim et al.'s (2014) study showed that the predictions of Att toward e-learning were statistically mediated by the subjective norms factor, and the prediction of BI was statistically mediated by perceived behavioral control. Findings in Seyal and Turner's (2013) investigation indicated that the Att factor had a positive relationship toward behavioral intention to use biometric technology, and factors such as Att, perceived behavioral control, behavioral intention, and actual use of BIO technology were determined by the subjective norms factor.

TAM, another theory drawn from TRA, emerged as a robust and widely accepted theoretical framework for explaining and forecasting the public's acceptance of IT (Bayaga &

Nyembezi, 2014). The original version of TAM postulates that users' actual use and behavioral intent to use a system can be explained by their perceptions of usefulness, ease of use, and attitude toward the system (Bagozzi, Davis, & Warshaw, 1989). In the TAM model, the perceived usefulness construct is grounded in the thought that the public has a propensity to accept or reject the use of a system to the degree that they expect the novel technology to help them improve their own performance (Bagozzi et al., 1989).

The perceived ease of use construct captures the viewpoint of the public that the use of a novel system will be uncomplicated (Bagozzi et al., 1989). Bagozzi et al. (1989) explained that perceived usefulness and perceived ease of use act as the foundation for individual attitudes regarding technology use, which, in turn, influences their behavioral intention of technology usage and triggers actual use. In addition, Bagozzi et al. (1989) indicated that external determinants intercede indirectly by having an effect on perceived usefulness and perceived ease of use. A recent literature analysis of over 80 scholarly articles with reference to TAM distinguished numerous extensions of the model to fit different technological settings, and showed that the notions of TAM have been supported by various investigations, highlighting its extensive applicability to a variety of IT systems (Granić & Marangunić, 2015).

Modifications of TAM have led to prominent theoretical extensions of the model. For instance, Taylor and Todd (1995) included subjective norms and perceived behavioral control factors from the TPB model in TAM to develop a decomposed theory of planned behavior. By combining TAM and TPB constructs, Taylor and Todd (1995) discovered that the BI factor was a significant predictor of the actual usage of technology for individuals with prior experience of the system. For first time users, the perceived usefulness and perceived ease of use factors were found to be strong determinants in predicting the BI to use the system (Taylor & Todd, 1995).

Additionally, Taylor and Todd's (1995) findings revealed that the perceived behavioral control factor influenced the BI factor for individuals with prior experience more than the perceived usefulness factor did.

To enhance the predictive strength of TAM, Davis and Venkatesh (2000) added more variables to TAM and developed TAM2, which is recognized as a successful theoretical extension of TAM (Abdollahzadeh, Ahmadi-Gorgi, Damalas, & Sharifzadeh, 2017). In Davis and Venkatesh's (2000) longitudinal investigation, subjective norms, image, job relevance, output quality, and result demonstrability were integrated into TAM and examined as determinants of perceived usefulness. The moderating effect of the experience and voluntariness factors on subjective norms was also evaluated (Davis & Venkatesh, 2000). In the TAM2 model, the image construct was grounded on a person's desire to maintain a positive reputation with others (Davis & Venkatesh, 2000). The job relevance construct indicated the extent to which the system was appropriate and the output quality denoted the degree to which the system satisfactorily operated according to its specifications (Granić & Marangunić, 2015). Finally, the result demonstrability variable represented how evident the advantages and functionality of the system was to users (Granić & Marangunić, 2015). Davis and Venkatesh (2000) examined TAM2 in both compulsory and non-compulsory situations and their findings provided empirical evidence supporting the assumptions of TAM2. Davis and Venkatesh's (2000) results were uniform, with the initial assumptions of TAM that the BI to utilize a system was significantly associated with the perceived usefulness and perceived ease of use factors.

In contrast to theories that sought to explicate a person's BI toward accepting a system, another standpoint was MPCU, which sought to explicate a person's actual use of a system, computers in particular (Higgins et al., 1991). According to MCPU, technology use behavior is

determined by factors such as “social norms, complexity of use, fit between the job and PC capabilities, and long-term consequences” (Higgins et al., 1991, p. 125). The MCPU also proposed that facilitating conditions factors and affective reactions to computers intervene directly, influencing a person’s actual use of a system, but Higgins et al. (1991) found that these factors were not significant predictors of system use.

MM is another theoretical model that has been used in research to explain the adoption and use of IT innovations (Bagozzi et al., 1992; Baroudi, Igarria, & Parasuraman, 1996; Bengtsson & Sällberg, 2016; Ifinedo, 2017). MM is based on the self-determination theoretical model, which underscored two key motivating forces: intrinsic and extrinsic (Deci & Ryan, 1985). From the perspective of the adoption and usage of IT innovations, Bagozzi et al. (1992) defined the intrinsic motivational factor as an individual’s inherent delight and joy to carry out an activity and the extrinsic motivational factor as the perceived usefulness, which indicated the individual’s incentive to carry out an activity because it generated a positive gain. Bagozzi et al.’s (1992) empirical investigation of MM as applied to the IT field revealed that both forms of motivation can predict and explain a person’s BI and use of a system. Bagozzi et al.’s (1992) results have been validated in several investigations that attempted to determine the impact of intrinsic and extrinsic motivations on the adoption of technologies, such as accounting information systems (Abduljalil & Zainuddin, 2015), online retail systems (Ahn, Han, & Ryu, 2007), and Internet-based learning mediums (Chen, Cheung, & Lee, 2005).

The DIT model formulated by Rogers (1962) is considered by many scholars to be a satisfactory approach for exploring the adoption of technological inventions and comprehending how an invention—that is, a novel notion, behavior, or system—diffuses within and between groups (Babalhavaeji, Khosravi, & Nazari, 2013; McGuire & Scott, 2017; Spil, Yan, Yu, &

Zhang, 2015). Rogers (2003) explained adoption as a person's decision to procure and use a novel technology, and described diffusion as the manner by which inventions disperse among communities as time passes. The DIT theoretical model posited that factors such as “(1) relative advantage, (2) compatibility, (3) complexity, (4) trialability, and (5) observability” increased or decreased the probability that the public would adopt a novel system (Rogers, 2003, p. 36). The first DIT factor is related to how people perceive the benefits of the novel system as being better than the technology it substituted (Rogers, 2003). The second factor referred to how uniform the novel system was in terms of principles, standards, know-hows, and requirements of potential users (Rogers, 2003). The third factor measured how challenging the novel system was to comprehend or operate (Rogers, 2003). The fourth factor examined the faculty of a novel system to be tested first before making a significant commitment or investment (Rogers, 2003). Finally, the fifth factor assessed the degree to which the novel system delivered noticeable results (Rogers, 2003).

Additionally, Rogers (2003) claimed that people have a tendency to accept an invention in a time succession, because people perceive the determinants of adoption in diverse manners. Rogers (2003) differentiated adopters of an invention into five classes: “innovators, early adopters, earlier majority, later majority, and laggards” (p. 298). Rogers (2003) described innovators as individuals who are willing to absorb novel notions and use the novel system first. Early adopters are typically knowledgeable about the novel system and they are prone to accept the new system very quickly (Spil et al., 2015). The earlier majority contains individuals that will accept the new system only if its advantages are clearly demonstrated (Rogers, 2003). In the later majority category, the public adopts the new system, but only after the vast majority of

users has tested it (Rogers, 2003). Finally, people in the laggards' category are traditionalist and resistant to adopting novel systems (Rogers, 2003).

Rogers (2003) postulated that technology acceptance was a cycle of proceedings that involve learning about the invention, being swayed to accept the invention because of the presumed advantages, deciding whether to accept the invention, putting into operation the invention, and corroborating the determination to accept the invention. From the perspective of the adoption of IT systems, Benbasat and Moore (1991) adapted Rogers's DIT model by separating the observability construct into two distinctive variables: "Result demonstrability and visibility," which relabeled complexity as ease of use, omitted trialability, and integrated image, and voluntariness (p. 210). According to Benbasat and Moore (1991), the result demonstrability construct not only assessed the degree to which the novel system generated noticeable results, but also the ability to disseminate them. The visibility construct evaluated the extent to which a person observed others utilizing innovative technology and images related to how people perceived that the utilization of the novel system enhanced their reputation (Benbasat & Moore, 1991). The use of DIT within the IT field supplied ways to evaluate the attributes of inventions and their influence on use. DIT takes into account public perceptions of the attributes of innovative systems as significant determinants that affect a person's decision to accept them (Ali & Wani, 2015).

The UTAUT theoretical model proposed by Davis et al. (2003) combined the above-mentioned theories with social cognitive theory (SCT) into a fused theoretical framework. Through longitudinal investigations, Davis et al. (2003) conducted a comparison and a conceptual and empirical examination of the resemblance of factors identified in each of the integrated theories that have an impact on BI and the use of technologies to build UTAUT (see

Appendix I). Davis et al.'s (2003) longitudinal investigations were carried out in four different businesses among workers in both compulsory and non-compulsory environments to predict their BI to adopt technologies. SCT was integrated into the model because it offered significant insights into what causes an individual to adopt specific conducts (Bandura, 1986).

Davis et al. (2003) found that the most influential constructs from the integrated theories were “performance expectancy, effort expectancy, social influence, and facilitating conditions” (p. 447). Davis et al. (2003) also identified “experience, voluntariness, gender, and age” (p. 467) as the most important moderators of constructs on BI to adopt technologies. Further, Davis et al.'s (2003) theoretical model accounted for 70% of the variance in BI to use technology. Since the establishment of the UTAUT model, numerous scholars have tested and demonstrated the validity of the model in predicting BI in different settings across a wide variety of technologies (Bytha, Khechine, Lakhal, & Pascot, 2014; Dowd, Joa, Magsamen-Conrad, & Upadhyaya, 2015; Weng, Wu, & Yu, 2012). Additionally, scholars argued that UTAUT offers a sturdy theoretical base for exploring user technology adoption and utilization (Bytha et al., 2014; Chauhan & Jaiswal, 2016; Gunawardena & Samaradiwakara, 2014).

Bytha et al.'s (2014) investigation examined undergraduate information technology (IT) students registered in a blended class at a Canadian university in Quebec in order to determine the critical factors influencing their decision to adopt a web conferencing system. Bytha et al.'s (2014) results supported Davis et al.'s (2003) assumptions that PE, SI, and FC had an impact on BI toward the system. Bytha et al. (2014) also showed that the effect of PE and FC were moderated by age, but there was no interacting effect with core determinants or gender. According to Bytha et al.'s (2014) research, the variance explained by their theoretical

framework with moderators increased to approximately 73% when compared to in examinations of UTAUT without moderating variables, which was approximately 51%.

Dowd et al. (2015) adopted Davis et al.'s (2003) UTAUT model to explore the acceptance of tablets among people of different ages and genders. Dowd et al.'s (2015) investigation reported that the effort expectancy and FC constructs had an impact on people's BI to use tablets and that age differences moderated the effects of effort expectancy and FC. However, Dowd et al. (2015) found minimum support for the effect of PE and SI constructs on BI and that there were no interacting effects with core variables or gender on intention. Moreover, in Dowd et al.'s (2015) study, the effort expectancy and FC factors only explained 24% of the variance in BI to use tablets when the moderating effects of age, gender, and experience were included. Although the variance reported in Dowd et al.'s study was much lower than for Davis et al.'s (2003) UTAUT model, Dowd et al.'s (2015) suggested that Davis et al.'s UTAUT model provided a robust foundation to examine the acceptance of novel technology across and within age groups.

Weng et al.'s (2012) empirical study conducted in Kaohsiung city among metro riders used Davis et al.'s (2003) original version of UTAUT to examine the determinants of Taiwanese people's adoption and use of a public transportation smart card known as the I Pass. Weng et al.'s (2012) findings backed up the importance of the effect of effort expectancy and SI on BI, demonstrated that FC and BI played a significant role in determining the utilization of I Pass, and confirmed that the effect of UTAUT constructs were moderated by experience, voluntariness, gender, and age. However, PE was not found to be a significant influence on public transport users' BI to use the I Pass (Weng et al., 2012). Weng et al. (2012) revealed interesting factors relating to individuals' anticipations of smart card technology in transportation systems and

made suggestions for the effective implementation of transport mechanisms with smart card ticketing schemes.

Other researchers have also applied the UTAUT model to examine various questions associated with technology adoption in the tourism industry (Carvajal-Trujillo & Escobar-Rodríguez, 2014), biometric technology in e-shopping (Hino, 2015), healthcare telemedicine equipment (Bush et al., 2014), and the use of a SNIC in Malaysia (Loo et al., 2013). Since UTAUT's legitimacy and soundness have been confirmed across a wide variety of innovations (Addo & Attuquayefio, 2014b; Hino, 2015; Loo et al., 2013; Miltgen et al., 2013), and the model has been suggested as a robust approach for comprehending user technology adoption (Bytha et al., 2014; Chauhan & Jaiswal, 2016; Gunawardena & Samaradiwakara, 2014), UTAUT can thus be seen as a satisfactory method for investigating the U.S. public's behavioral intention to use CBIOSCT.

Versions of UTAUT. Studies on the acceptance and use of IT have distinguished numerous versions of UTAUT to fit diverse technological settings (Addo & Attuquayefio, 2014a; Dwivedi, Rana, & Williams, 2014). Some investigators have claimed that UTAUT, notwithstanding its extensive validation, needs to be expanded in order to provide a more thorough comprehension of IT acceptance. In a recent systematic analysis, Addo and Attuquayefio (2014a) examined 20 investigations using UTAUT or other extensions of the model to explicate technology adoption. Addo and Attuquayefio (2014a) discovered that the determinants of IT acceptance or use often differed across countries, settings, and technologies. Another literature analysis of 174 studies using UTAUT found that PE and BI remained significant predictors of technology acceptance behavior (Dwivedi et al., 2014). Moreover, Dwivedi et al. (2014) found that most investigations of UTAUT focused on the acceptance of

technologies within the context of electronic commerce, electronic government, online banking, and online learning. Dwivedi et al. (2014) urged further investigation of the model with more variables across various contexts and innovations in order to identify more factors, which could also potentially become significant predictors of technology acceptance and use.

An assortment of UTAUT theoretical perspectives on the acceptance and use of technologies have identified some important predictors of BI: Att (Gaffar et al., 2013); compatibility, privacy, trust, perceived risk, and innovativeness (Miltgen et al., 2013); hedonic motivation (Louw, Madigan, Merat, Schieben, & Wilbrink, 2017); and PC (Loo et al., 2013). Gaffar et al. (2013) integrated the Att variable into UTAUT to study factors that could influence the acceptance of mobile learning among Guyanese college students, and indicated that this adaptation increased the predictive power of the model. Miltgen et al. (2013) integrated UTAUT, TAM, and DIT theoretical models and other determinants, such as innovativeness, trust, privacy, and risk perceptions, into their investigation on the BI to accept and recommend BIO technology. Miltgen et al. (2013) showed the significant influence of compatibility, perceived usefulness, FC, privacy, trust, innovativeness, and risk on BI. However, SI and perceived ease of use had no influence on BI.

Louw et al.'s (2017) enhanced UTAUT model included the construct of hedonic motivation—delight in an innovation—to examine Greeks' BI to adopt automated road vehicles among citizens of Trikala. Louw et al. (2017) found that adding hedonic motivation augmented the power of the whole study and pointed out that although the construct of effort expectancy did not influence BI, the other constructs of hedonic motivation, PE, SI, and FC were significant determinants of BI to adopt driverless transport.

Loo et al. (2013) examined the impact of PE, PC, SI, FC, and anxiety on Malaysian citizens' BI to adopt a national identity SC, using a version of UTAUT. Loo et al.'s (2013) results showed PE and PC as direct determinants of BI and indicated that the prediction of the PE variable was mediated by the PC variable. Loo et al. (2013), in their pioneering investigation, explained that further research focusing on how users accept a SC technology based on the roles it is created to support is needed.

Since the focus of this study is on providing a better understanding of the issues surrounding the U.S. public's BI to adopt CBIOSCT, and the extensive literature on technology adoption identifies UTAUT as a prominent model (Bytha et al., 2014; Chauhan & Jaiswal, 2016; Gunawardena & Samaradiwakara, 2014), the UTAUT theory was applied. Investigations in the area of BIO and SC technology adoption have been limited compared to investigations in the acceptance of other technological innovations (Loo et al., 2013; Seyal & Turner, 2013). In an empirical analysis, Morosan (2016) developed a theoretical model that mixed UTAUT with privacy concerns and compatibility to explicate U.S. air passengers' BI to use BIO electronic gates. Morosan (2016) revealed a significant impact of effort expectancy on PE and identified PE as a direct determinant of intention to use BIO electronic gates. Furthermore, Morosan (2016) explained that, although privacy concerns and compatibility did not have a significant influence on BI, these constructs remained essential but weak predictors of U.S. air passengers' BI.

Another approach to examine BIO technology adoption suggested incorporating perceived privacy and PC as direct determinants of BI in the UTAUT model and analyzing the moderating effects of age, gender, and experience (Hino, 2015). Exploring online consumers' BI to utilize BIO technology in online shopping, Hino (2015) discovered that BI was determined by

PC, privacy, PE, and SI. Hino (2015) also showed that the effect of perceived privacy and PC were moderated by experience, but there was no interacting effect from core determinants or age and gender.

The main phenomena that investigations on biometrics have in common are the use or adaptation of UTAUT (Davis et al., 2003), and every single investigation attempted to identify and explain the public's acceptance and use of innovative systems. The purpose of the above-mentioned investigations was to enhance technology provisions for consumers hinged on their perceptions. Notwithstanding the diverse settings in which the different examinations were conducted, the aforementioned investigations offered advantageous and important data that contributed to this investigation.

Influencing factors. Loo et al.'s (2013) pioneering investigation, which evaluated Malaysian citizens' acceptance of a SNIC for homeland security, explained that further research focusing on how users accept a SC technology based on the roles it is created to support is needed. To determine the factors that shape the U.S. public's acceptance of CBIOSCT, the investigation framework used Loo et al.'s (2013) extension of UTAUT to include PE, PC, SI, and FC as independent variables, and expanded the model to include Att as another independent variable. The aforementioned variables were identified as essential elements in determining the level of approval towards the use of CBIOSCT (Bush et al., 2014; Loo et al., 2013; Morosan, 2016; Seyal & Turner, 2013).

The variable of anxiety, proposed by Loo et al. (2013), was not included, since stress or nervousness does not arise from using CBIOSCT when technology adoption is voluntary. According to Davis et al. (2003), the anxiety factor has an indirect effect on BI through effort expectancy. The effort expectancy factor was also excluded in this investigation, since using

CBIOSCT requires no time or effort: participants will only carry the card and present it to legal entities upon request. Further, according to Tao, Wu, and Yang (2007), the effort expectancy construct may be used to predict intention to use a system, but it may not perform well in predicting BI to adopt a technology. Thus, the anxiety and effort expectancy constructs were judged as not applicable.

Dowd et al. (2015) described PE as the extent to which people anticipated that their work-related activities would progress with the use of a particular technology. Numerous scholars have demonstrated this factor as a keen predictor of the adoption of technologies, such as home telehealth services (Brenčič, Cimperman, & Trkman, 2016), biometric authentication in e-shopping (Hino, 2015), a Malaysian SNIC (Loo et al., 2013), and mobile learning (Mtebe & Raisamo, 2014). The PE construct encompasses a combination of five different predictors in the adoption of technology: “perceived usefulness (TAM/TAM2 and C-TAM-TPB); extrinsic motivation (MM theory); job-fit (the model of PC utilization); relative advantage (innovation diffusion theory), and outcome expectations (social cognitive theory)” (Davis et al., 2003, p. 447) (see Appendix I).

In this investigation, PE represented the extent to which the U.S. public anticipates that using CBIOSCT will limit their chances of becoming the target of identity thieves. According to Loo et al.’s (2013) findings, the PE of a Malaysian SNIC centers on its PC, which in turn, influences Malaysians’ intention to use it. To determine if the same phenomenon applied to CBIOSCT, the extent to which the prediction of BI, as measured by the PE scale, was statistically mediated by PC was examined.

Hwang, Lee, and Shin (2017) defined PC as the degree to which individuals believe that a technology is secure, robust, and reliable, and could be trusted (Hwang et al., 2017; Loo et al.,

2013). Scholars have suggested that credibility is associated with privacy (Hino, 2015) and technology safety concerns (Loo et al., 2013). Specific areas of worry embraced the appropriateness of safety measures for collection, safekeeping, and handling of information (Carpenter, Chen, Hicks, & Maasberg, 2016), as well as confidence in the system's defense mechanisms, accuracy, and reliability (Hwang et al., 2017). Empirical studies have supported the notion that PC influences individuals' intention to adopt and utilize technology, such as Internet banking systems (Ariff, Ishak, Ismail, Min, & Zakuan, 2013), biometric technology in e-applications (Hino, 2015), health informatics (Hwang et al., 2017), and a Malaysian SNIC (Loo et al., 2013). Therefore, in line with the previous literature, PC was operationalized in this investigation as the extent to which the U.S. public expects that CBIOSCT will be a secure system in which data is kept confidential, is handled securely and effectively, and is difficult to forge and modify.

The SI variable refers to the perception that somebody who holds a meaningful position in someone's lives thinks he or she should accept and use the system (Dowd et al., 2015). Various scholars have suggested that a person's determination to engage in a particular behavior is often affected by image (Chauhan & Jaiswal, 2016), social pressure (Loo et al., 2013), superiors, relatives (Martins, Oliveira, & Popovič, 2014), and peers (Mtebe & Raisamo, 2014). Empirical investigations have supported the notion that SI is a determining factor in a person's willingness to use technology, such as e-learning (Dečman, 2015), business intelligence systems (Hou, 2014), or social media (Harsono & Suryana, 2014). In light of the previous literature, SI in this investigation measured whether or not the U.S. public's intention to utilize CBIOSCT is influenced by the views or motivation of someone who holds a meaningful position in their lives.

Chauhan and Jaiswal (2016) indicated that FC described the degree to which a specialized, administrative, and technological structure was present to reinforce technology acceptance. Investigations predicting individuals' willingness to use technology have incorporated FC as a meaningful predictor, since the existence of adequate infrastructure promotes the use of technology (Brenčić et al., 2016; Chauhan & Jaiswal, 2016; Harsono & Suryana, 2014). However, other scholars have disagreed, stating that FC has no direct impact on the adoption and use of technology (Martins et al., 2014). Notwithstanding the volatile function of FC in prognosticating technology acceptance and usage, FC is considered by numerous scholars to be a valuable factor in explaining what encourages people to adopt and use technologies (Gaffar et al., 2013; Loo et al., 2013; Mtebe & Raisamo, 2014). Therefore, in this investigation, FC represented the extent to which the U.S. public considers that the existence of a specialized, administrative, and technological structure facilitates the acceptance and use of CBIOSCT.

Harsono & Suryana (2014) outlined the BI construct as a reflection of how willing people are to adopt and use a system. According to Seyal and Turner (2013), intents are presumed to describe the driving forces behind a person's behavior and to denote the degree to which people are willing to execute the behavior. Numerous investigations have demonstrated that BI is directly affected by PE, PC, SI, FC, and Att (Hino, 2015; Hwang et al., 2016; Loo et al., 2013; Seyal & Turner, 2013). In this investigation, BI measured the extent to which the U.S. public is willing to adopt and use CBIOSCT.

Even though Att, which refers to the person's postures of approval or disapproval (Seyal & Turner, 2013), is not an explicit construct in the UTAUT framework, for the purposes of this investigation, Att was considered to be an essential element in determining the level of approval

toward the use of CBIOSCT. Other scholars have studied the effect of attitude on biometric adoption and have proposed that this construct is also a predictor of acceptance and intent to use a technology (Seyal & Turner, 2013). According to Seyal and Turner (2013), the Att factor indicates positive or negative responsive behaviors to using technologies. Previous investigations have incorporated Att in the UTAUT framework to assess its correlations with the UTAUT constructs. For instance, Gaffar et al. (2013) indicated that Att is positively correlated with PE, FC, and effort expectancy factors and that Att has a direct effect on the adoption and use of technology.

Hwang et al. (2016) suggested that Att correlates with PE and has a significant impact on people's intention toward the use of a novel system. Davis et al. (2003) suggested that when PE and effort expectancy are excluded from the UTAUT framework, the effect of Att should be considered instead. In this investigation, the effort expectancy factor was omitted since CBIOSCT is very simple to use: the cardholder shows an ID at someone's request. Thus, the absence of effort expectancy allowed Att to be incorporated. In light of the previous literature, Att in this investigation represented the extent to which the U.S. public favors or disfavors the adoption and utilization of CBIOSCT in current forms of ID in the United States for identity theft and fraud prevention.

Identification systems. In the United States, there is no countrywide mandated form of identification; instead, federal, state, and local governments provide various papers and credentials to identify civilians. The most widely utilized documents include birth, marriage, or divorce certificates; passports or passport ID cards; Social Security (SS) cards; DoD ID cards; green cards; driver's licenses; and state ID cards (Agbaraji, Agwah, & Ezetoha, 2014; Hu, 2013). Although not all identification documents bear a photo of the holder, all of them contain some of

the holder's PII. Customary types of PII include the holder's name, address, birthdate, demographic data, SSN, and biometric information, such as fingerprints or a photograph (Andrus, 2017). Some identification documents may also contain an embedded chip, magnetic stripe, or barcodes (Devadas & Meng-Day, 2017).

Self-identification means little without evidence to support that claim (Wiehl, 2012). Identity authentication is an essential and legal prerequisite to exercise entitlements to reside, vote, and work in a certain place and to use services in the public and private sectors (McGrath, 2016). For instance, a birth certificate provides evidence of the holder's nationality, and is an essential proof of identity when applying for an SSN, a passport, a driver's license, a state ID card, or for school registration (Agbaraji et al., 2014; Fagnäs, 2014). Marriage or divorce certificates are required papers to verify a person's name change (Brooks, 2013). In the case of foreign nationals married to U.S. legal residents, a marriage certificate and, if remarried, a divorce decree is necessary to apply for a marriage-based green card (U.S. Citizenship and Immigration Services [USCIS], 2016). Furthermore, people who have lost their spouses may use a death certificate to provide evidence of the spouse's death to claim SS benefits, life insurance, or burial arrangements (Randall, 2014).

A U.S. passport, implanted with a RFID microchip, is required to travel abroad (Jung & Lee, 2015) and is a valid document for verification of identity and nationality when applying for an SSN (Social Security Administration, n.d.), a driver's license, or a state ID card (New York State Department of Motor Vehicles, 2017). An SS card contains the holder's legal name and personal identification number (PIN) (Social Security Administration, n.d.). The PIN displayed on the SS card is needed to file taxes, conduct financial transactions, claim SS benefits, obtain some federal and state services, corroborate a candidate's employment eligibility, and access

employment-related files (Electronic Privacy Information Center, n.d.). The DoD ID card, also known as the CAC card, is the accepted form of identification for the U.S. Armed Forces, DoD civilians, and DoD contractors (DoD, 2014). CAC technology provides a more rigorous way of confirming and validating the cardholder's identity, since it is used in conjunction with a personal identification number (PIN), public key infrastructure (PKI) authentication tools, personal identity verification (PIV) certificates, and biometric technology (DoD, 2014).

A green card is an ID document that serves to authenticate the identity of a foreign national who has lawful permanent resident status (USCIS, 2017). A green card contains information, such as the holder's legal name, identification number, nationality, birthdate, digital photo, and fingerprint, along with embedded holographic images and an RFID tag (Renaud, 2016). Finally, a driver's license or a state ID card are also valid forms of identity verification. State ID card holders cannot use this type of identification to drive; however, the public and private sectors broadly use both forms of identification to confirm the identity of a person conducting business with commercial, government, and financial institutions (Agbaraji et al., 2014). Additionally, state governments use driver's licenses and state ID cards to locate sex felons (Bonnar-Kidd, 2010), to prevent underage alcohol consumption (Fell, Romano, Scherer, & Taylor, 2015), and to locate child support evaders (National Conference of State Legislatures, 2017a).

Many of the previously mentioned identification mechanisms have been a focal point for identity criminals to steal, counterfeit, and misuse (Copes, Pike, Powell, & Vieraitis, 2015). A recent study conducted by Kessler International (2015) revealed that counterfeit documents have become too easily accessible and inexpensive since the Internet facilitates the selling of fake documentation across borders. Kessler International (2015) also discovered that all safety

measures and design details used in official documents can be imitated by criminals, who make the counterfeit document look truly authentic. Various scholars suggest that the use of counterfeit papers represents an omnipresent offense that is typically associated with terrorism, identity theft, and organized crime (Agbaraji et al., 2014; Baechler et al., 2013; Copes et al., 2015).

In the United States, Congress enacted the Real ID ACT of 2005, to prevent extremists and felons from obtaining identification documents, such as driver's licenses or state ID cards (Martin, Wallace, & Walton, 2015). Another aim of this legislation was to enhance the trustworthiness, soundness, and precision of identification cards issued by the states (Martin et al., 2015). To issue these types of enhanced ID documents, states are required to confirm the authenticity of the papers provided by applicants with the issuing organization for determination of state-issued ID cards' eligibility (Real ID Act, 2005). Additionally, all states must institute measures to detect counterfeit documents and share DMV records between them (Real ID Act, 2005). According to Martin et al. (2015), all state-issued enhanced ID cards must have a RFID microchip and must show the holder's official name, birthdate, gender, PIN, home address, signature, and facial biometric identification.

Critics of the Real ID Act have claimed that the benefits of this legislation are minimal compared to the danger of identity theft victimization, since criminals could potentially breach the DMVs' systems and plunder their databases (Kravitz, 2009; Thiessen, 2008). Others argue that the Real ID Act is a method for carrying out surveillance, since the RFID technology facilitates officials in tracing a person's whereabouts by pursuing the locations where the enhanced state-issued ID card has been used (Electronic Privacy Information Center, 2017; Hu, 2013). To prevent disapproval of the legislation, supporters of enhanced state-issued ID cards

avowed that the Real ID Act is indispensable in thwarting illegal immigration, averting terror attack plots, and diminishing ID fraud (Real ID Act Proceedings and Debates, 2005). In fact, this law was enacted in response to the terrorist acts of September 11, 2001, in which attackers used fake papers and valid state-issued ID cards to move freely throughout the United States without raising concern or suspicion (Miller, 2016).

The Transportation Security Administration (TSA) stated that, during the middle of January 2018, licenses and identification cards issued by states that are noncompliant with the Real ID's standards could not be used as a valid form of ID for national flights (DHS, 2016b). Further, the DHS announced that beginning in the fall of 2020, noncompliant state-issued licenses and ID cards would not be a valid form of ID for entering federal buildings (National Immigration Law Center, 2016). At this time, DHS has identified four states as noncompliant, granted extensions to 26 states and jurisdictions, and recognized 26 regions as compliant with the Real ID's criteria (DHS, 2017).

The requirements that DHS expects from each state and jurisdiction to be considered compliant with the Real ID Act include a proposed security design to safeguard and manage DMVs' physical and logical security (Real ID Act, 2005). Specifically, the design must explain the physical defense mechanisms on the Real ID card, describe the safety measures to achieve security policies and procedures, protect the storage and handling of records, control access to buildings and assets, deter threats, and address vulnerabilities and incidents (Real ID Act, 2005). A recent study indicated that compliant states that are already issuing EDL and EID cards use a centralized system and implemented a public awareness campaign, and most of them provide applicants with a temporary ID while their supporting application documents are authenticated.

After application for EDL or EID is approved, customers receive the EDL or EID card by mail (Martin et al., 2015).

Ho and Ni (2008) suggested that the existence of so many forms of identification in the United States makes it challenging to authenticate an individual's identity, since the identification documents are handled and stored by various organizations that do not have direct connectivity between their equipment to share data. Consequently, the lack of assurance about information integrity raises worries over identity theft and fraud. Ho and Ni (2008) highlighted the need for an efficacious and methodical ID mechanism in the United States that permits organizations to harmonize processes, connect identity information for authentication, identify identity thieves, and deter identity fraud schemes.

Identity theft and identity fraud. Identity theft and identity fraud are expressions used to denote the illegal acquisition of someone else's PII—such as passwords, private data, PINs, or security tokens—for the purpose of impersonating the victim to commit or attempt to commit criminal acts or for personal financial gain (Jamieson et al., 2012). Some popular techniques used by identity thieves include spying on other people as they complete a document, using an automated teller machine (ATM), or using other automated gadgets to obtain PII (Kwon, Na, & Shin, 2014). Identity thieves may also look for PII in dumpsters or mailboxes (Bradbury, 2016) or use advanced technologies or online schemes to extract the victim's PII (Clough, 2015).

Identity criminals may use the victim's PII to purchase fake ID cards or merge victims' PII with the perpetrator's information to sell counterfeit ID cards (O'Leary, 2014). For instance, in the United States, law enforcement officials at John F. Kennedy International Airport confiscated more than 4000 fake identification documents made in China between 2013 and 2014 (Fliegelman, 2015). Bradbury (2016) explained that United Kingdom police forces have

captured information resellers with portable ID card-making equipment, who were selling fake driver's licenses out of the trunks of their cars. In general, identity thieves use victims' PII to buy property, merchandise, goods, and services, to take control of the targeted individual's financial credit or savings, to obtain jobs, loans, and credit cards, or to pose as the victim for felonious purposes (DOJ, 2015).

According to the ITRC (2017), in 2016, there were 1,093 data breaches in the United States, which represents a significant increase of 40% from the 780 breaches reported in 2015. These breaches exposed more than 36 million records and included information such as Social Security Numbers (SSNs), health reports, drivers' license numbers, passport numbers, addresses, credit and debit cards numbers, and bank statements.

Some recent punishments for identity theft and fraud examples include a four-year imprisonment and a restitution fine of about \$100,000 imposed on a man in California for using hundreds of identity theft victims' PII to file bogus tax returns and cash refund checks (Internal Revenue Service [IRS], 2016) and two identity crooks serving a prison term of two years and three months in Puerto Rico for illegally buying and selling Puerto Ricans' PII. Federal prosecutors have said that the criminals were using the Puerto Rican identity theft victims' PII to assume the victims' identities, to perpetrate financial crimes, and to acquire valid driver's licenses and U.S. passports throughout the United States (IRS, 2017).

Recently, the Federal Trade Commission (FTC) (2017) identified the five most popular types of identity theft: tax fraud, financial deception, utility bill scams, loan and leasing scams, and federal ID cards or benefits schemes. Additionally, the FTC (2017) revealed that, although accusations of identity theft decreased 3% in 2016 from the 16% reported in 2015, identity theft victims' accusations of credit card deception have more than doubled since 2015, increasing by

33%. The precise number of people victimized by identity theft is difficult to establish since victims often do not discover the identity crime until a couple of months after it happened (Indermaur, Roberts, & Spiranovic, 2013). Other causes of delay include identity theft victims' reluctance to notify law enforcement officials (FTC, 2017) or their unawareness due to some companies' unwillingness to notify customers of data breaches for fear of deteriorating customers' level of trust (Clough, 2015).

Legal reaction. Identity theft is a challenging behavior to tackle (Hsieh, Lai, & Li, 2012); however, recent studies have demonstrated that the enactment of legislation addressing this issue has curtailed incidents of identity theft. An investigation assessing the effect of enacted "data breach disclosure" legislation revealed a 6.1% decrease in the theft of PII cases related to incidents of data breaches (Acquisti, Romanosky, & Telang, 2011). Another study demonstrated that state implementation and enforcement of stipulations in "data breach notification" statutes diminishes identity theft offenses (Maniff & Sullivan, 2016). In the United States, various state and federal laws punish identity crimes. For instance, in Puerto Rico, Guam, Washington, DC, and 27 states, identity felons are penalized with restitution fines for identity theft and identity fraud-related losses (National Conference of State Legislatures, 2017b). Moreover, several states have increased criminal and financial punishments against those targeting senior citizens or people with disabilities (Kluwer, 2015).

In the federal government, there is no specific statute to address recognition and detection of identity crimes, but there is a wide variety of laws that tackle incidents of identity theft and protect affected victims. The statutes that address identity crime offenses include The Identity Theft and Assumption Deterrence Act (ITADA) of 1998, The Fair Credit Reporting Act (FCRA, 1970), the Fair and Accurate Credit Transactions Act (FACTA) of 2003, the Fair Debt Collection

Practices Act (FDCPA, 2010), the ITPEA of 2004, and the Identity Theft Enforcement and Restitution Act (ITERA) of 2008 (DOJ, 2010). In an effort to deter identity theft, identity fraud, and the misuse of victims' PII, ITADA brands these types of offenses as federal crimes (ITADA of 1998). Additionally, ITADA appointed the FTC to receive accusations of identity crimes and to synchronize their response proceedings with law enforcement officials, to capture, convict, and incarcerate identity crooks (Kluwer, 2015).

The FCRA statute created rules about the validity and confidentiality of credit reports. FACTA is a modification of FCRA, bolstering and enhancing the safeguards for people directly affected by identity theft (DOJ, 2010). FACTA section 114 directs creditors and financial institutions to develop strategies and procedures to tackle identity theft. Likewise, section 112 mandates that Consumer Reporting Agencies (CRA) and creditors provide recovery assistance to individuals impacted by incidents of identity theft (FACTA, 2003). Recovery support services must include a fraud alert on the credit record of the affected person, an annual credit report at no cost, and an examination of victims' dispute claims to amend all erroneous information related to their incidents of identity theft (Kluwer, 2015).

The FDCPA legislation forbids individuals and businesses from using dishonest or unjust ways to collect overdue debts (FDCPA, 2010). If a person impacted by identity theft has reported this offense to CRAs, FACTA section 154 forbids debt collectors from reselling, trading, or reassigning the overdue account (FACTA, 2003), whereas FDCPA section 805(c) restricts further attempts to collect the debt (FDCPA, 2010). ITPEA, on the other hand, institutes penalties for serious offenses of identity theft, such as using someone else's PII to purchase or sell fake ID cards, counterfeiting government documents, or enacting fraud, financial deception, government benefits scams, terrorism felonies, or immigration delinquencies (ITPEA of 2004).

Finally, ITERA established penalization and restitution fines for identity theft offenders, permitting courts to take legal action against identity theft felons residing in the jurisdiction where the affected person lives (ITERA of 2008). Under this legislation, identity thieves must make payments to those directly impacted by identity crimes. The restitution penalty takes into consideration both the time devoted to repairing the harm caused and the direct damage instigated by the robbery (Kluwer, 2015).

Other legislation that has been enacted to safeguard civilians' PII, which helps to diminish incidents of identity theft: The Driver's Privacy Protection Act (DPPA) of 1993, the Family Educational Rights and Privacy Act (FERPA) of 1974, the GLBA of 1999, and Health Information Portability and Accountability Act (HIPAA) of 1996 (DOJ, 2010). DPPA provides limitations on what PII the Department of Motor Vehicles (DMV) across the United States can release about users (DPPA, 1993). Likewise, FERPA provided restrictions on what educational files or information schools across the United States receiving federal aid can release about students (FERPA, 1974). Under GLBA, financial institutions must comply with several requirements, including the mandatory use of security safeguards to protect consumer data from unauthorized disclosure, access, misuse, loss, or alteration (GLBA, 1999). Finally, HIPAA regulates the disclosure, safekeeping, and privacy of patients' health data (HIPAA, 1996).

Financial institution reaction. Organizations in the financial sector use a wide range of devices, tools, procedures, and software to minimize expenses and occurrences of identity theft. These consist of practices such as the identification of first-time clients, verification of existing clients, and the recognition of deceitful and ambiguous transactions (Lott, 2015). The identification of first-time clients is vital to creating continuous rapport, wherein a large part of all future financial dealings can be completed with client information already acquired by the

business. The identification process entails meticulous substantiation of fundamental forms of identification, such as a driver's license, a state ID card, a DoD ID card, and/or an SSN (Lott, 2015). Today, many corporations use authentication services that contrast data from the credentials shown at the requested time to data stored in various database systems. For example, numerous financial institutions use checking systems, such as "ChexSystems and Early Warning," to verify new and existing clients' PII and screen them for prior cases of scam or deception (Friedline, 2016).

Typically, existing clients' identities are validated by inputting known information, such as their correct password, PIN, SSN, date of birth, and/or secret word. Likewise, by presenting valid credentials such as their bank card or SC or by inputting their fingerprints or facial images for accurate validation (Hemphill & Longstreet, 2016). According to Bertino, Huang, Xiang, Xu, and Zhou (2014), a multifactor validation scheme that depends on the aforementioned identity validation components is the most effective method for confirming identity and to safeguard information. To recognize deceitful and ambiguous transactions, financial institutions take preventative steps, such as implementing data analysis tools, rules to filter ambiguous and deceitful bank account activities, and transactions alerts (Bănărescu, 2015; Joyner, 2011). Dash and Mishra (2014) indicated that one of the most effective and broadly used methods for detecting fraudulent transactions is an artificial neural network (ANN), due to its ability to locate patterns and irregularities concealed in substantial amounts of information.

Additionally, creditors and business in the financial sector must fulfill the red flag rule requirements enacted under the FACTA statute in their efforts to combat identity theft (Kunick & Posner, 2011). Red flag rule directives instruct the aforementioned organizations to devise tailor-made policies and measures for validating the identity of the person undertaking or trying

to carry out the transaction and for safeguarding classified clients' information from incorrect or deceitful use (Kunick & Posner, 2011). Yücel (2013) indicated that the establishment of red flag guidelines can be a valuable tool for organizations, since these rules operate as an "early warning system" to uncover and deter fraud (p. 154). The FTC Identity Theft Rules (2007) also instructs creditors and business in the financial sector to frequently evaluate the aptness of current validation and safeguarding methods and keep them up-to-date as new vulnerabilities emerge.

Consumer reaction. Combating identity crimes, such as theft and fraud, is not only essential for organizations, but also for clients. Scholars have indicated that people behave differently in warding off and discovering ID crimes (Cleveland, Hille, & Walsh, 2015). Conventional coping and technological coping conduct have been demonstrated to be valuable mechanisms for combating identity crimes (Cleveland et al., 2015). Conventional coping refers to an individual's typical way of acting to safeguard PII, and technological coping refers to an individual's way of acting to safeguard PII when using computers (Cleveland et al., 2015). Some of the conventional defense mechanisms individuals exhibit in averting ID theft consist of maintaining password confidentiality, limiting the sharing of PII on social networks, and monitoring and destroying credit reports, financial and medical records, and bank and credit card statements (FTC, 2012). In the technological context, Hedayati (2012) highlighted the importance and necessity of changes in user conduct by following prevention tactics, such as the use of anti-malware programs, the installation of firewalls, keeping the operating system updated, and maintaining browser protections.

Since identity criminals are continuously learning and improving their skills in order to be successful (Copes et al., 2015), individuals must apply various security measures to protect their PII. Archer and Gilbert's (2012) study about users' identity crime prevention and detection

conduct revealed that users tend to use only one type of detection and prevention conduct, which can produce substantial costs for users. Therefore, Archer and Gilbert (2012) urged individuals to use numerous defensive strategies to diminish the likelihood of identity crime occurrence and the negative impact of identity theft and identity fraud. Users have a crucial responsibility in safeguarding their PII; negligence or inattentiveness to secure their PII can nullify the identity theft and fraud deterrent efforts of authorities and organizations.

Combined biometric and smart card technology (CBIOSCT). The rate of identity theft and fraud is rising every day (ITRC, 2017), affecting societies around the world, and, lamentably, it is not a problem that will end anytime soon (Cassim, 2015). In an effort to combat identity crimes and make societies safer, governments around the globe are embracing authentication mechanisms with CBIOSCT (Agbaraji et al., 2014). An SC offers an effective system that is secured and cannot be sabotaged to store PII and authentication data. Some of the attributes of SCs include: “match-on-card biometric, on-card cryptographic processing chip, and on-card digital signing and encryption” (Al-Khoury, 2013, pp. 225-226). The use of CBIOSCT has vastly expanded around the world. The applications of this technology include identity verification and validation, banking, storage and data management, access control, mobile communications, public transport payment, Internet safety, and security (Sweta, 2015).

The use of SCs and biometric systems has been described and evaluated in numerous ways, including concerns about privacy in the workplace (Carpenter et al., 2016), uses for crime deterrence (Pocs, 2013), responses to user perceptions and behavior (Loo et al., 2013), and benefits as an effective component of a countrywide ID system (Benjamin, Emmanuel, & Franklin, 2014). Furthermore, extant investigations on the topic have concentrated on either user perceptions of biometric technology (Harinda & Ntagwirumugara, 2015; Miltgen et al., 2013;

Morosan, 2016) or both SC and BIO technology in mandatory settings (Fahl, Harbach, Smith, & Rieger, 2013; Loo et al., 2013).

However, there has been little analytical work done on the issues surrounding the adoption of CBIOSCT in current forms of ID in the United States for identity theft and fraud prevention in voluntary settings. Loo et al. (2013) suggested that researchers study the issues surrounding the adoption of ID systems with an embedded technology similar to the Malaysian SNIC. Various scholars and organizations are confident that a convergence of BIO and SC technologies can effectively authenticate and verify the identity of an individual (Das et al., 2014; Karuppiah & Saravanan, 2014; Li et al., 2015a), but, so far, there is little understanding of the problems associated with the acceptability of the intersection of these technologies. Therefore, there is a need for research to comprehend the determinants associated with the acceptability of BIO and SC technologies for combating identity theft and fraud in the United States in order to devise strategies, policies, and procedures that will warrant effective implementation and adoption of a combined biometric smart card (CBIOSC).

Smart cards with BIO technology use an embedded microchip that can store and process large amounts of data (Ching-Wei et al., 2015). According to Li et al. (2015a), CBIOSCs offer a safe and convenient authentication or identification of a person, since they are difficult to forge. In countries such as Argentina, Belgium, Brazil, Germany, Portugal, and the United Kingdom, the key driving forces for the inclusion of a chip in their national ID cards were national security, fraud and crime protection, the prevention of counterfeit identification, and to make government services more effective for their citizens (Council of the European Union, 2010; Fascendini & Roveri, 2014; FEDICT, 2012; Soares, 2011).

In the United States, numerous bills have been introduced in Congress in the midst of concerns about identity crimes. One bill proposes a social security SC with BIO technology (Social Security Identity Theft Prevention Act, 2008). The Real ID Act (2005) would implement CBIOSCT for drivers' licenses and state ID cards to increase homeland security. Another bill would mandate a Medicare smart card with biometric identifiers to minimize fraud, enhance protection, and bolster and privacy (Medicare Common Access Card Act, 2015). The GAO (2016) conducted a thorough review of hundreds of healthcare fraud cases and found that smart cards are a pioneering solution to avert fraud. Nonetheless, numerous studies argue that BIO systems and ID card programs with BIO technology are an intrusion of privacy and cause exploitation, as they could be converted into mechanisms of surveillance (Alonso-Bejarano & Goldstein, 2017; Bozbeyoğlu, 2011; Donovan & Martin, 2015; Hu, 2013; McGrath, 2016; Poliang & Yung-hua, 2016).

For instance, Alonso-Bejarano and Goldstein (2017) debated whether E-Verify, the authentication system that incorporates BIO technology to determine an individual's work authorization, as required by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), is a type of surveillance. Since the E-Verify system corroborates the information provided by the job seeker in the I-9 employment eligibility form against data that is stored in DHS and SS administration databases, Alonso-Bejarano and Goldstein (2017) explained that this promotes racism, invades privacy, and sparks fear among immigrants searching for jobs. The E-Verify system recognizes forged SS numbers and categorizes job applicants by their eligibility to work legally in the U.S.; this type of classification marginalizes and labels documented and undocumented immigrant applicants and increases their fear of

surveillance and deportation, wage theft, and unfair treatment (Alonso-Bejarano & Goldstein, 2017).

Some studies on BIO technology for identification systems have found that the surveillance of private information is escalating through ID programs (Bozbeyoğlu, 2011), that governments misunderstand how citizens perceive the use of BIO technology (Hosein, Martin, & Whitley, 2014), and that governments' stated intentions to use BIO technology are unclear and misunderstood by citizens (Donovan & Martin, 2015). Various scholars concur that the triumph or failure of technology initiatives depends, in part, on public perceptions. As Brown et al. (2016) asserted, the public's interest in using BIOs is an important aspect of the successful implementation of such technology. Having doubts about the government's true reason for implementing CBIOSCT in ID programs can lead to user resistance and may undermine an otherwise well-devised technology-based initiative (McGrath, 2016). Po-liang and Yung-hua (2016) agreed with McGrath (2016) that the public needs to be informed about how CBIOSCT will be executed before an advanced ID program begins. But Po-liang and Yung-hua (2016) noted that, for some users, acceptance of CBIOSCT depends more on their aspirations for a sturdy government structure to uphold "social order" and "welfare" than on the potential threats or doubts that CBIOSCT could garner (p. 259). Despite the privacy and security concerns associated with a CBIOSCT ID program, building credibility and confidence among citizens has been characterized as decisive factors in CBIOSCT acceptability by numerous scholars (Donovan & Martin, 2015; Kamis et al., 2011; McGrath, 2016).

Building credibility and confidence in CBIOSCT requires governments to offer a trustworthy identification system with a strong layer of defense against theft and misuse of citizen information (McGrath, 2016). A strong layer of defense refers to the certainty that the

CBIOSCT scheme is equipped with numerous measures to protect its infrastructure and performance against each possible attack vector (Li et al., 2015b). Identity verification systems with CBIOSCT can be at risk of being compromised by attacks such as denial-of-service (DoS), forgery, imposture, or smart card thievery (Das et al., 2014; Li et al., 2015b). A DoS attack occurs when an individual with a legitimate ID is mistakenly denied service or access as the result of a variation in the biometric characteristic of the person being authenticated (Das et al., 2014). For example, if the individual's facial image in the database lacks glasses, and at the time of authentication the person is wearing glasses, this slight variation can influence the accuracy of the facial recognition system (Borza, Danescu, & Darabant, 2013). Other categories of intrusion can result from internal or external attackers who may use stolen SCs to impersonate real users or use the extracted data from stolen SCs to perpetrate forgery attacks by creating illegitimate login credentials (Das et al., 2014; Li et al., 2015b).

CBIOSCT, then, needs to have adequate protection to minimize the risk of compromised information and prevent attacks from occurring (Li et al., 2015b). Belanche-Gracia et al. (2015) indicated that a well-secured system is a crucial requirement to reassure SC users that the technology is reliable and safe. Consequently, several scholars have suggested that the negative performance expectations that individuals have about the system are an additional factor hindering its broad use and acceptance (Hino, 2015; Loo et al., 2013; Mtebe & Raisamo, 2014). A recent study disclosed that current users with high-performance expectancy of the utilization of ID cards with an embedded integrated circuit chip, or SCs, are likely to have positive attitudes toward the adoption of technology and their intention to use it (Loo et al., 2013). These users expected that the technology would operate according to its specifications with minimal risk of threat (Loo et al., 2013).

Furthermore, the acceptance of technology hinges on user perception of its effortlessness and enhanced protection and public understanding of the value-added services and design system (Bush et al., 2014). Approval may also be influenced by social pressure and the risk of penalties, banning, punishments, or restrictions for non-participants (Seyal & Turner, 2013). For example, with the Real ID ACT EDL and EID card rule, people in the United States are required to have an EDL or EID to enter any federal agency (DHS, 2016a). To increase the chances of success and adoption of novel technologies, developers must have a general understanding of user needs, concerns, attitudes, and motivations (Bush et al., 2014), since technology advancements not only resolve issues for the agency developing them but also for the individuals using them.

Users might find an identity verification technology that offers benefits, such as identity theft and fraud prevention, to be useful if it relieves them of the stress that can underlie any of these issues. Cleveland et al. (2015) discovered that the fear of the theft of private information has an effect on consumer behavior. Hughley and Jator (2014) revealed that numerous health organizations have implemented BIOs systems to verify each patient's and each employee's identity to curtail healthcare fraud. Although the technological and design attributes of a system that play a role in its success are essential, it is valuable to study whether a recommended resolution is related and applicable to the issue it is intended to resolve. Ehteshami (2017) suggested that even very successful technological resolutions may end up being unacceptable if user perception and adoption barriers are not taken into consideration when first assessing the solution.

Summary

In the United States, many of the existing identification mechanisms have been a focal point for identity criminals to steal, counterfeit, and misuse (Copes et al., 2015). Kessler

International (2015) revealed that the acquisition of counterfeit documents has become too easily accessible and inexpensive since the Internet facilitates the selling of fake documentation across borders. Various scholars suggest that the use of counterfeit papers represents an omnipresent offense that is typically associated with identity theft, and organized crime (Copes et al., 2015).

To safeguard consumers' PII, Congress has passed acts to tackle issues surrounding identity theft and fraud, including the ITPEA of 2004, the GLBA of 1999, and the REAL Identification (ID) Act of 2005 (DOJ, 2010). The GAO (2016) conducted a thorough review of hundreds of healthcare fraud cases and found that smart cards are a pioneering solution to avert fraud. Nonetheless, numerous scholars have noted that the triumph or failure of technology initiatives depend, in part, on public perception. As Brown et al. (2016) asserted, the public's interest in utilizing BIOs is an important aspect of the successful implementation of such technology. Loo et al.'s (2013) investigation, which evaluated Malaysian citizens' acceptance of a smart national ID card for homeland security, explained that further research is needed and should focus on how users accept a SC technology based on the roles it is created to support.

A major theoretical concept of technological adoption explaining how individuals come to accept and use a system is UTAUT (Davis et al., 2003). Since UTAUT's legitimacy and soundness has been confirmed across a wide variety of innovations (Hino, 2015; Loo et al., 2013; Miltgen et al., 2013), using UTAUT is seen as a satisfactory method to investigate the U.S. public's behavioral intention to use CBIOSCT. Without a better understanding of the factors influencing user acceptance of BIO and SC technologies, the private and public sectors' precise strategies, policies, and procedures to put into operation, for vast adoption of a CBIOSC for identity theft prevention, are undetermined. The methodology and design of the investigation are discussed in detail in the next chapter.

Chapter 3: Research Methods

The escalation of identity theft and fraud has become a major source of concern for people and U.S. law enforcement agencies (Cassim, 2015). The number of people affected by identity theft rose from 13.1 million victims in 2015 to 15.4 million victims in 2016 (Marchini et al., 2017). In addition, over the last six years, U.S. identity theft victims have lost about \$107 billion (Marchini et al., 2017). A strategy being adopted in many countries to detect and deter identity theft and fraud is the implementation of a smart national identity card (SNIC) (Identity Systems, 2017; Loo et al., 2013). However, people's refusal to adopt and use individual authentication technologies is identified as a failure factor in CBIOSCT implementation (Miltgen et al., 2013). Thus, the need for further examination of factors associated with the acceptability of BIO and SC technologies for combating identity theft and fraud is warranted.

Various scholars and organizations are confident that a convergence of BIO and SC technologies can effectively authenticate and verify the identity of an individual (Das et al., 2014; Karupiah & Saravanan, 2014; Li et al., 2015a), but, so far, there is limited research into the factors associated with the adoption of these technologies. Some investigators have used technology acceptance theories to examine public intent to use BIO technology on a voluntary basis, and have suggested that the public's willingness to adopt and use BIO technology is affected by their perceptions of its FC, the PE of these mechanisms (Hino, 2015; Miltgen et al., 2013), and their Att toward the technology (Seyal & Turner, 2013). Other studies that have examined the public's acceptance of technology in a mandatory environment have confirmed the appropriateness of technology acceptance models to determine user adoption and willingness to use such a system (Dečman, 2015; Loo et al., 2013). These studies have also found social

influence (Dečman, 2015) and perceived credibility (Loo et al., 2013) to be important determinants of the acceptance of technology.

The problem addressed in this investigation is the need for further examination of factors associated with the acceptability of BIO and SC technologies for combating identity theft and fraud. Without a better understanding of the factors influencing user acceptance of BIO and SC technologies, the private and public sectors' precise strategies, policies, and procedures to put into operation, for adoption of a combined biometric smart card (CBIOSC) for identity theft prevention, would be undetermined. Loo et al. (2013) evaluated Malaysian citizens' acceptance of a smart national ID card for homeland security and explained that further research focusing on how users accept a SC technology based on the roles it is created to support is needed.

As a result, the aforementioned problem led to the purpose of this nonexperimental correlational quantitative investigation: to examine the relationship between the independent variables of performance expectancy (PE), perceived credibility (PC), social influence (SI), facilitating conditions (FC), and attitude (Att) on the dependent variable of the U.S. public's behavioral intention (BI) to use CBIOSCT, including the extent to which the predictions of PE are mediated by the PC variable. Research instrument items were adapted based on earlier investigations using UTAUT (Loo et al., 2013) and its added components (Bush et al., 2014; Morosan, 2016). Additionally, the study survey was adapted from Loo et al.'s original questionnaire (2013) and modified to fit the investigative context (see Appendix A). Online questionnaires were distributed through SurveyMonkey (see Appendix B) among SurveyMonkey respondents who were residents of New York, NY; Washington, CD; Orlando, FL; Charleston, SC; Las Vegas, NV; and San Francisco, CA to assess the factors that impact the U.S. public's

acceptance of CBIOSCT. The following six research questions were based on the study purpose and the research conceptual framework of the UTAUT model:

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT?

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT?

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT?

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT?

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT?

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility?

After providing a synopsis of the research purpose, this chapter continues the discussion about the design and methodology of the investigation. It begins with a discussion of the investigative scheme designed to address the research problem. Then, the discussion moves to a description of the methodology, which consists of the population and sample, the materials and instrumentation, the operational definition of the variables, study procedures, data collection, and data analysis. Finally, the discussion turns to the investigation's assumptions, limitations, delimitations, and ethical assurances.

Research Methodology and Design

The objective of this nonexperimental, correlational, investigation was to examine the relationship between the independent variables of PE, PC, SI, FC, and Att on the dependent variable of the U.S. public's BI to use CBIOSCT, including the extent to which the predictions of PE were mediated by the PC variable. This investigation sought to provide a further understanding of the issues surrounding the U.S. public's intention to adopt and use CBIOSCT for identity theft and identity fraud prevention. This quantitative approach was the most favorable option since it has been the primary method utilized in several BIO technology acceptance investigations: Chieh-Heng and Chun-Chieh (2015) used it to evaluate hotel employees' perceptions and adoption of BIO systems; Hino (2015) used it to examine the factors that influence web users' behavioral intent to utilize BIO technology in electronic commerce; and Miltgen et al. (2013) used it to study the factors associated with the acceptability of BIO technologies.

Gunaydin and McCusker (2015) explained that a quantitative investigation methodology allows data to be gathered utilizing deep-rooted methods and previously validated tools and allows it to be examined via statistical analysis to produce valid results. Additionally, applying the same analytical methods to examine larger samples under similar settings (Gunaydin & McCusker, 2015) allows for this investigation to be replicated and the information to be evaluated and compared to similar technology acceptance research. According to Park and Park (2016), a quantitative methodology is appropriate when the scholar attempts to detect and segregate specific constructs within the research framework by establishing causality and other correlations between and among constructs. Furthermore, Cano et al. (2014) suggested a nonexperimental, correlational, quantitative approach if the scholar is assessing constructs in

their original form with no manipulation, and SEM or another method of statistical analysis is used to portray and measure the extent to which two or more constructs are associated and when there is no random allocation of subjects to groups.

Various scholars (Claydon, 2015; Garza & Landrum, 2015; Park & Park, 2016) have explained that when the aim of the study is to uncover further knowledge or develop new theoretical concepts and notions to explicate a phenomenon, the choice of a qualitative approach is justified. However, if the aim of the investigation is to test and verify theories and their individual assumptions to generalize and replicate the results in other subjects and environments, a quantitative method is most suitable (Claydon, 2015; Park & Park, 2016). To conduct this investigation, other quantitative approaches, such as ex post facto, experimental, and quasi-experimental (Leedy & Ormrod, 2013) were taken into account, but not selected.

The ex post facto and quasi-experimental approaches were not chosen because these involve placing participants into groups (Leedy & Ormrod, 2013), and the experimental approach was not chosen because it entails manipulation of an independent variable (Aguinis & Bradley, 2014), which is not feasible in this investigation. Hence, a nonexperimental, correlational, quantitative approach was most fitting to conduct this investigation since none of the independent variables (PE, PC, SI, FC, and Att) were manipulated to identify their influence on the dependent variable BI. Moreover, there was no random allocation of subjects to groups, and this study tested the mediation of predictability for the predictor construct of PE by the mediating construct of PC predicting the dependent variable of BI.

The data was gathered using an online survey devised to assess the perspectives of the subjects. The study survey format was adapted from Loo et al.'s (2013) original questionnaire and administered to 100 randomly selected SurveyMonkey audience members residing in each

city—New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA—for a total of 600 surveys. Leedy and Ormrod (2013) indicated that “when the desired sample size is quite large, an online questionnaire is far more cost-effective than a mailed questionnaire” (p. 206). In addition to cost savings, the online survey method used in this nonexperimental correlational quantitative investigation enhanced the possibility for each of the participants to respond to questions at their own pace, participate in a low peer-pressure context, skip any question, or end their participation at any time without penalty or prejudgment (Williams, 2012).

Likewise, using an online survey tool and panel was the best choice because it is the most robust and prominent tool in scholarly investigations (Balasubramanian et al., 2017; Elbeck, 2014) and it aligns well with recent studies on technology adoption: Horrey et al., (2017) constructed the research questionnaire via SurveyMonkey and administered it to respondents via Amazon Mechanical Turk to evaluate the predictive relevance of TAM, TPB, and UTAUT to explicate motorists’ behavioral intent to use an Advanced Driver Assistance System (ADAS). Balasubramanian et al. (2017) distributed questionnaires and gathered responses via SurveyMonkey to examine Asian Indians’ intention to use mobile shopping applications.

Research instrument items were adapted based on earlier investigations using UTAUT (Bush et al., 2014; Loo et al., 2013; Morosan, 2016) to provide a better understanding of the factors influencing the public’s acceptance and adoption of novel technologies. All scales in the measurement instrument were integrated and slightly modified to fit the U.S. context from validated questionnaires that have been demonstrated to be valid and reliable for assessing user intentions and acceptance in other environments (Bush et al., 2014; Loo et al., 2013; Morosan, 2016) (see Appendix A). The measurement instrument of this investigation did not put

respondents at risk of harm since the confidentiality of respondents remained intact by keeping the online survey anonymous with no names, phone numbers, or emails collected.

Questionnaires were distributed only after receiving approval from NCU's IRB. Each construct in this investigation was assessed in the survey instrument by three items measured using a five-point Likert scale response format ranging from 1 - Strongly Disagree to 5 - Strongly Agree (see Appendix A). The survey questionnaire included demographic information, producing a profile of respondents and ordinal questions, in order to measure participants' opinions about CBIOSCT. In this investigation, all results were tested using a SEM technique and SPSS AMOS software. The mediation of predictability for the predictor construct of PE by the mediating construct of PC predicting the dependent variable of BI was also tested using linear regression. A regression analysis is appropriate when testing the strength of relationship between constructs (Lewis, Saunders, & Thornhill, 2015). The SEM statistical procedure and SPSS AMOS software were a suitable approach since both have been used in a number of relevant research projects. For example, Loo et al. (2013) applied SEM and AMOS to investigate the ergonomic problems influencing the public's decision in Malaysia to use a countrywide ID card, Addo and Attuquayefio (2014b) used SEM and SPSS AMOS to study "the issues surrounding acceptance of ICT by students of tertiary Institutions" (p. 75), and Al-Abdallah and Al-Qeisi (2014) employed SEM and AMOS to analyze the components of website design influencing users' use of the system.

Population and Sample

The possible population for the investigation consisted of U.S. persons, 18 years of age and older, who are legally eligible for a U.S. driver's license or a state identification card and reside in any of the 50 states. For the calendar year 2016, the U.S. Census Bureau (2016)

estimated that the United States had a total resident population age 18 year and older of 249,485,228. A recent study revealed that 15.4 million people were victimized by identity fraud in the United States in 2016 (Marchini et al., 2017). This population was outlined to correctly exhibit the large U.S. population from which the sample was selected. Since the investigation required that the research site be comprised of residents of the most visited cities by tourists throughout the United States, due to the ease with which incidents of security such as theft, domestic, international, and cross-border terrorism could occur (Mansfeld & Pizam, 2006), the population available for the investigation was reduced substantially. Therefore, the investigation was delimited to people residing in New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA. These cities were selected from the ranking of U.S. cities most visited by tourists (TripAdvisor, 2016).

Due to the boundary condition described above for the investigation, selection of participants was based on a nonprobabilistic, purposeful sampling. The core objective of a nonprobabilistic purposive sampling method is to reach the intended population, which in turn, best enables the scholar to answer the questions posed (Hao-Hsien, Hui-Man, & Lee-Jen, 2014). This method allowed for selecting respondents that met the following criteria: 18 years of age and older, legally eligible for a U.S. driver's license or a state identification card, and residing in New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA. Although a nonprobabilistic, purposive sample was not a true generalizable representation of the U.S. public's behavioral intention to use CBIOSCT, research findings offered important insight into understanding the U.S. public's perspectives of CBIOSCT at multiple tourist destinations throughout the United States.

A total of 600 surveys were disseminated through SurveyMonkey to randomly selected SurveyMonkey respondents residing in each of the above-mentioned cities. Various scholars have explained that SurveyMonkey panels reach a wide-ranging diverse pool of valid respondents of as many as thirty million audiences, and have pointed out that “benchmarking surveys” are conducted by SurveyMonkey on a regular basis to make certain that their respondents’ demographic features are comparable to the U.S. population (Berg et al., 2017, p. 193).

To make sure that the sample size selected was representative of the population, a power analysis for the Chi-square (X^2) test of goodness-of-fit was conducted to determine the minimum sample size required to detect a statistically significant effect. The power analysis was set to the X^2 family of tests, the goodness-of-fit tests, and the *a priori* analysis to calculate the sample size needed. The alpha level, the power, and the effect size were set as follows: $\alpha = .05$, $\beta = .80$, effect size $f^2 = .30$, with 1 degree of freedom (df; the number of restrictions in the model) (Miles, 2003, p. 3). Further, a medium effect size was set according to Cohen’s standards (Cohen, 1992). These elements of power calculations were set based on similar investigations that have demonstrated an appropriate use of study (Addo & Attuquayefio, 2014b; Allen et al., 2014). After the above-mentioned parameters were input, it was determined that a minimum sample size of 88 was required to have an optimum probability of rejecting false null hypotheses (see Appendix E). Since a total of 600 online surveys were distributed, it was expected that the total of responses was greater than 88, as this attained a coveted true report probability (Kaelin, Kallischnigg, Vuillaume, & Weitkunat, 2010).

Materials/Instrumentation

Research instrument items were adapted from earlier investigations utilizing UTAUT (Loo et al., 2013) and its added components (Bush et al., 2014; Morosan, 2016) to provide a further understanding of the factors influencing the public's acceptance and adoption of novel technologies (see Appendices F–H). It was anticipated that the survey would be concluded in no more than 15 minutes. The survey questionnaire in this nonexperimental, correlational, quantitative design included three sections using a nominal and ordinal scale of measurement, adapted with permission from Loo et al. (2013). The first section investigated demographic information to produce a profile of the respondents. Demographic questions, adapted with permission from Loo et al. (2013) and Morosan (2016) (see Appendices F & G), included age, gender, education level, and annual household income. From Loo et al.'s (2013) survey instrument, race, nature of occupation, and monthly income level were excluded, and city of current residence and driver's license or state ID card eligibility questions were added to fit the investigation objectives. The second section assessed PE, PC, SI, FC, and Att. Finally, the third section measured intent to use CBIOSCT in existing forms of personal identification in the United States. Constructs in the last two sections were presented to participants in question form using a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, and 5 – Strongly Agree (see Appendix A).

The PE and PC scales adapted from Loo et al. (2013) consisted of three items in each scale. The items included in the performance expectancy scale, measured the extent to which participants perceive that CBIOSCT is useful for identity theft and identity fraud prevention as well as effective identity verification and authentication. The items included in the PC scale measured the extent to which CBIOSCT is perceived as being difficult to forge, being secure,

and limiting unauthorized access to users' personal information. The scale for SI, adapted with permission (see Appendix F) from Loo et al. (2013), included three items that measured the extent to which participants perceive whether people who are important to them, individuals they know who use the technology, or the government influence(s) their intentions to use CBIOSCT. The second social factor, "most Malaysians have applied for MyKad SNIC" (Loo et al., 2013, p. 727), was not applicable. Instead, the item—"people I know who are using CBIOSCT at their workplace influence my intention to use"—was added to the instrument to represent social influence SI2.

The scale for FC, constructed with permission and based on the work of Loo et al. (2013), included three items that measured the extent to which participants perceive that enabling components exist to encourage the acceptance of CBIOSCT. Enabling components consisted of the availability of CBIOSCT infrastructure in the United States' public and private sectors for identity authentication and fraud risk detection, the availability of a customer service contact center in case of any questions relating to CBIOSCT, and the discontinuation of current driver's licenses and state ID cards embedded technology. The second FC factor in Loo et al.'s (2013) survey instrument was excluded since it did not fit this investigation context. Loo et al.'s (2013) anxiety instrument was also not included in this investigation's measurement model since the anxiety factor was considered inapplicable to the research objectives.

The scale for Att—adapted with permission from scholars (see Appendices F–H)—was included to measure the extent to which participants perceive that using CBIOSCT is a good idea, beneficial, and enhances their standard of living (Bush et al., 2014). Finally, the scale for intention to use—adapted from Loo et al. (2013)—included three items measuring the extent to

which participants in the future will use CBIOSCT for identification purposes and for identity theft and fraud prevention.

All scales were integrated and slightly modified to fit the U.S. context from validated questionnaires used by other scholars (Bush et al., 2014; Loo et al., 2013; Morosan, 2016). In various studies, other scholars have also demonstrated that the instruments used in this investigation are reliable and valid for assessing users' intentions and acceptance in other environments (Ali, El-Masri, Serrano, & Tarhini 2016; Moeser & Moryson, 2016; Šorgo & Šumak, 2016). Bastos, Bonamigo, Duquia, González-Chica, and Mesa (2014) recommended that scholars using a pre-existing instrument ensure that it suits the research objectives to produce correct data for examination. G. Sullivan (2011) recommended that researchers use instruments that already exist, since their reliability and validity have been consistently demonstrated in replicated examinations.

The variables under study—PE, PC, SI, FC, Att, and BI—were measured using a five-point Likert scale response format (see Appendix A). Loo et al. (2013) reported that a reliability coefficient alpha above .7 indicates an acceptable reliability of the measure, a Pearson coefficient below .8 suggests that the “inter-construct correlations” (p. 724) do not present multicollinearity issues, and an Average Variance Extracted (AVE) with a value above of .5 indicates a good convergent validity of the measure. Likewise, Loo et al. (2013) explained that discriminant validity is demonstrated by corroborating that the square roots of the AVE values are larger than “the inter-construct correlations” (p. 724), and content validity is established by documenting a thorough and critical literature examination of the constructs under investigation. In Loo et al.'s (2013) measurement model, the coefficient Cronbach's alpha for PE is .8, PC is .75, and BI is .71. The AVE value for PE is .64, PC is .6, and BI is .69. The square root of AVE for PE is .8,

for PC is .77, and for BI is .83, and the inter-construct Pearson correlations for PE and PC are .41, PE and BI are .62, and PC and BI are .62.

Loo et al. (2013) omitted FC and SI constructs from the examination, because the confirmatory factor analysis (CFA) revealed that the items included in the FC and SI constructs had loading scores below .7. Even though Loo et al.'s (2013) measurement model indicates a low loading value for FC and SI constructs, FC and SI factors were kept in this investigation; other studies have found these factors to deliver high values of alpha and have demonstrated their validity. For instance, in a study of the factors influencing patients and healthcare personnel to use telemedicine systems, Bush et al. (2014), used a CFA to determine the validity of each construct. According to Bush et al. (2014), a comparative fit index (CFI) with a minimum value of .9, a root mean square error of approximation (RMSEA) value below .08, a research instrument item with a loading larger than .7, and a ratio value lower than 2 of a Chi-square given the change in degrees of freedom (X^2/df) indicate a satisfactory model with good convergent and discriminant validity. In Bush et al.'s (2014) investigation, the CFI was .924, the RMSEA was .79, the ratio of X^2/df was 1.8; the factor loading for SI was .883 and FC is .914; and the reliability coefficient alpha of SI was .865, FC was .801, and BI was .941. Bush et al. (2014) added the Att construct to the UTAUT design and demonstrated its reliability and validity, reporting a reliability coefficient alpha of .872 and loadings for each Att item of .8.

Other scholars investigating the factors affecting mobile learning acceptance at a university in Guyana reported a reliability coefficient alpha of .789 for SI and .797 for FC, a convergent and discriminant validity with an AVE value of .622 for SI, square roots of AVE of .789 for SI, .649 for FC, and .872 for BI, and inter-construct correlations for FC and BI of .582 and SI and BI of .524 (Gaffar et al., 2013). For FC items, Gaffar et al. (2013) reported an AVE

value of .42, which fails to show a satisfactory convergent validity, because it is below the recommended .5. To address this limitation, Gaffar et al. (2013) used the third FC item loading of .779 to surmount the construct in estimated designs. Additionally, when the effect of Att on BI is considered in the UTAUT design, Gaffar et al. (2013) reported a RMSEA of .052 and a CFI of .967, an AVE value of .776 for Att, and square roots of AVE of .88 for Att, which demonstrates a satisfactory design with good convergent and discriminant validity. Similarly, Seyal and Turner (2013) demonstrated the reliability and validity of the Att construct by reporting a reliability coefficient alpha of .909, a convergent validity with an AVE value of .648 for Att, and a discriminant validity for the Att factor with a larger AVE value of .648 than the R-squared coefficient of determination of .344 for the Att factor, and an AVE value of Att larger than the highest R-squared of .532 among the constructs.

Operational Definitions of Variables

The survey questionnaire in this nonexperimental, correlational, quantitative design included three sections, using a nominal and ordinal scale of measurement adapted from Loo et al. (2013). The first section investigated demographic information to produce a profile of respondents. Demographic questions adapted from Loo et al. (2013) and Morosan (2016) included age, gender, education level, and annual household income. The second section assessed the independent variables: PE, PC, SI, FC, and Att. Finally, the third section measured the dependent variable: BI to use CBIOSCT in existing forms of personal identification (see Appendix A). This section provides a description of the operationalization of the dependent and independent variables used in this investigation.

Performance expectancy (PE). PE is the extent to which people anticipate that their work-related activities will progress with the use of a particular technology (Dowd et al., 2015).

Numerous scholars have demonstrated that this factor is a predictor of the adoption of technologies, such as home telehealth services (Brenčič et al., 2016), biometric authentication in e-shopping (Hino, 2015), a Malaysian SNIC (Loo et al., 2013), and mobile learning (Mtebe & Raisamo, 2014). PE encompasses a combination of five different predictors in the adoption of technology: “perceived usefulness (TAM/TAM2 and C-TAM-TPB); extrinsic motivation (Motivational Model); job-fit (the model of PC utilization); relative advantage (innovation diffusion theory), and outcome expectations (social cognitive theory)” (Davis et al., 2003, p. 447) (see Appendix I).

In this investigation, PE represented the extent to which the U.S. public anticipates that utilizing CBIOSCT will limit their chances of becoming the target of identity bandits. PE was measured as an independent variable, based on Loo et al.’s (2013) questionnaire scale and as derived from participants’ opinions to three items using an ordinal scale. Each of the three items used a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, and 5 – Strongly Agree (see Appendix A).

According to Loo et al.’s (2013) findings, the public PE of a Malaysian SNIC centers on its PC, which in turn, influences Malaysians’ intention to use. To determine if the same phenomenon applied to CBIOSCT, the extent to which the prediction of BI, as measured by the PE scale, was statistically mediated by PC was investigated. The items included in the PE scale measured the extent to which the U.S. public believes that utilizing CBIOSCT will protect them against identity theft (PE1), enhance the reliability of their personal data and thus protect them against identity fraud (PE2), and allow for an effective identity verification and authentication process (PE3).

Perceived credibility (PC). PC is the degree to which individuals believe that the technology is secure, robust, reliable, and can be trusted (Hwang et al., 2017; Loo et al., 2013). Scholars have suggested that credibility is associated with privacy (Hino, 2015) and technology safety concerns (Loo et al., 2013). Specific areas of concern embrace the appropriateness of safety measures for collection, safekeeping, and handling of information (Carpenter et al., 2016), as well as confidence in the system's defense mechanisms, accuracy, and reliability (Hwang et al., 2017). Empirical studies support the notion that perceived credibility influences individuals' intention to adopt and use technology, such as Internet banking systems (Ariff et al., 2013), biometric technology in e-applications (Hino, 2015), health informatics (Hwang et al., 2017), and a Malaysian SNIC (Loo et al., 2013).

In line with the previous literature, PC was operationalized in this investigation as the extent to which the U.S. public expects that CBIOSCT will be a secure system in which data is kept confidential, handled securely and effectively, and is difficult to forge and modify by criminals. PC was measured as an independent variable, based on Loo et al.'s (2013) questionnaire scale and as derived from the participants' opinions regarding three items on an ordinal scale. Each of the three items used a five-point Likert scale response format ranging from 1 –Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, and 5 – Strongly Agree (see Appendix A). The items included in the PC scale measured the extent to which CBIOSCT is perceived as being difficult to forge (PC1), secure (PC2), and limiting unauthorized access to users' personal information (PC3).

Social influence (SI). SI refers to the perception that somebody who holds a meaningful position in someone's lives thinks he or she should accept and use the system (Dowd et al., 2015). Various scholars suggest that a person's determination to engage in a particular behavior

is often affected by image (Chauhan & Jaiswal, 2016), social pressure (Loo et al., 2013), superiors, relatives (Martins et al., 2014), and peers (Mtebe & Raisamo, 2014). Empirical investigations have supported the notion that SI is a determining factor of a person's willingness to use technology, such as e-learning (Dečman, 2015), business intelligence systems (Hou, 2014), or social media (Harsono & Suryana, 2014).

In light of the previous literature, SI in this investigation measured whether or not the U.S. public's intention to utilize CBIOSCT is influenced by the views and motivation of someone who holds a meaningful position in their lives. Moreover, SI was measured as an independent variable, adapted from Loo et al.'s (2013) questionnaire scale and as derived from participants' opinions to three items using an ordinal scale. Each of the three items used a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, and 5 – Strongly Agree (see Appendix A). The items included in the SI scale measured the extent to which participants perceive that the people who are important to them (SI1), individuals they know who use the technology (SI2), or the government (SI3) influence their intentions to use CBIOSCT.

Facilitating conditions (FC). FC describes the degree to which a specialized, administrative, and technological structure is present to reinforce technology acceptance (Chauhan & Jaiswal, 2016). Investigations predicting individuals' willingness to use technology have incorporated FC as a meaningful predictor, since the existence of adequate infrastructure promotes the use of technology (Brenčič et al., 2016; Chauhan & Jaiswal, 2016; Harsono & Suryana, 2014). However, other scholars have disagreed and stated that FC have no direct impact on the adoption and use of technology (Martins et al., 2014). Notwithstanding the volatile function of FC in prognosticating technology acceptance and usage, numerous scholars

have considered FC to be a valuable factor in explaining what encourages people to adopt and use technologies (Gaffar et al., 2013; Loo et al., 2013; Mtebe & Raisamo, 2014).

In this investigation, FC represented the extent to which the U.S. public considers that the existence of a specialized, administrative, and technological structure facilitates acceptance and use of CBIOSCT. FC was measured as an independent variable, constructed based on the work of Loo et al. (2013), and derived from participants' opinions to three items using an ordinal scale. Each of the three items used a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, to 5 – Strongly Agree (see Appendix A). The FC factor included three items that measured the extent to which participants perceive that enabling components exist to encourage acceptance of CBIOSCT. Enabling components consisted of the availability of CBIOSCT infrastructure in the United States' public and private sectors for identity authentication and fraud risk detection (FC1), the availability of a customer service contact center to respond to questions related to CBIOSCT (FC2), and the expectation that current driver's licenses and state ID cards embedded technology are likely to be phased out soon (FC3).

Attitude (Att). The Att factor indicates a person's positive or negative responsive behavior to the use of technologies (Seyal & Turner, 2013). Previous investigations have incorporated Att in the UTAUT framework to assess its correlations with UTAUT constructs. For instance, Gaffar et al.'s (2013) findings indicated that Att is positively correlated with PE, FC, and effort expectancy factors and that Att has a direct effect on the adoption and use of technology. In a recent study, Hwang et al. (2016) suggested that Att correlates with PE and has a significant impact on people's intention towards the utilization of a novel system. Davis et al. (2003) suggested that when PE and effort expectancy are excluded from the UTAUT framework,

the effect of Att should be considered instead. In this investigation, the effort expectancy factor is omitted since CBIOSCT is very simple to use: the cardholder shows an ID at an agency's request. The absence of effort expectancy allows Att to be incorporated. Various scholars have also considered Att to be a valuable factor in explaining BI (Gaffar et al., 2013; Hwang et al., 2016; Seyal & Turner, 2013).

In light of the previous literature, Att represents the extent to which the U.S. public favors or disfavors the adoption and use of CBIOSCT. Att was measured as an independent variable, adapted from Bush et al.'s (2014) questionnaire scale and as derived from participants' opinions to three items on an ordinal scale. The Att factor included three items that measure the extent to which participants perceive that using CBIOSCT is a good idea (Att1), is beneficial (Att2), and enhances their standard of living (Att3). Each of the three items used a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, to 5 – Strongly Agree (see Appendix A).

Behavioral intention (BI). BI explains how willing people are to adopt and use a system (Harsono & Suryana, 2014). According to Seyal and Turner (2013), intents are presumed to describe the driving forces behind a person's behavior and to denote the degree to which people are willing to execute the behavior. Numerous investigations have demonstrated that BI is directly affected by PE, PC, SI, FC, and Att (Hino, 2015; Hwang et al., 2016; Loo et al., 2013; Seyal & Turner, 2013). In this investigation, BI measured the extent to which the U.S. public is willing to adopt and use CBIOSCT. Additionally, BI was assessed as a dependent variable adapted from Loo et al. (2013) and as derived from participants' opinions to three items using an ordinal scale. BI included three items measuring the extent to which participants in the future will adopt and use CBIOSCT for identification purposes (BI1), predict utilization of CBIOSCT

for identity theft and fraud prevention (BI2), and continue to use CBIOSCT for identity theft and fraud prevention (BI3). Each of the three items used a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, to 5 – Strongly Agree (see Appendix A).

Study Procedures

This nonexperimental, correlational, quantitative investigation examined the relationship between the independent variables of PE, PC, SI, FC, and Att on the dependent variable of the U.S. public's BI to use a CBIOSCT in current forms of identification for identity theft and identity fraud prevention. To determine the factors that shape the U.S. public's acceptance of the CBIOSCT, the investigation framework utilized Loo et al.'s (2013) extension of UTAUT: PE, PC, SI, and FC while expanding the model to include Att (see Figure 1). The study survey format was adapted from Loo et al.'s (2013) original questionnaire. Moreover, all scales in the measurement instrument were integrated and slightly modified to fit the U.S. context from questionnaires that have been demonstrated to be valid and reliable for assessing users' intentions and acceptance in other environments (Bush et al., 2014; Loo et al., 2013; Morosan, 2016) (see Appendix A).

The measurement instrument of this investigation did not put respondents at risk of harm. To protect the confidentiality of respondents, the online surveys remained anonymous with no names, phone numbers, or emails collected. Surveys were distributed only after receiving approval from NCU's IRB. After obtaining authorization, participants were randomly selected from the SurveyMonkey audience. They received a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D) explaining the purpose of the study, the safety measures taken to ensure anonymity, the data handling procedures, and a notice that their

participation was voluntary. Additionally, SurveyMonkey never makes audience members' PII accessible to anyone, including researchers.

Data Collection and Analysis

In this nonexperimental, correlational, quantitative investigation, the survey questionnaire included three sections using a nominal and ordinal scale of measurement adapted with permission from Loo et al. (2013). The first section investigated demographic information to produce a profile of the respondents. The second section assessed PE, PC, SI, FC, and Att. Finally, the third section measured intention to use CBIOSCT in existing forms of personal identification. Constructs in the last two sections were presented to participants in question form using a five-point Likert scale response format ranging from 1 – Strongly Disagree, 2 – Disagree, 3 – Neither Agree nor Disagree, 4 – Agree, and 5 – Strongly Agree (see Appendix A).

Conducting national-scale investigations are costly and time-consuming (Bell & Ramsey, 2014); therefore, the site for the intended investigation was delimited to residents of the top six most visited cities by tourists throughout the United States, according to TripAdvisor. The selected cities were divided by region as follows: two located in the Northeast, New York, NY and Washington, DC; two located in the Southeast, Orlando, FL and Charleston, SC, and two located in the West, Las Vegas, NV and San Francisco, CA. These cities were selected from the importance ranking of U.S. cities most visited by tourists (TripAdvisor, 2016).

One hundred online questionnaires (see Appendix B) were disseminated through SurveyMonkey among randomly selected SurveyMonkey respondents residing in each of the above-mentioned cities for a total of 600 surveys. Each subject received a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D) with a link to the survey, explaining the purpose of the study and the safety measures taken to ensure anonymity.

On the informed consent form, in the signature section, it was explained that by clicking “Yes”, participants consented to answering the questions in the survey. By answering all questions in the survey, respondents implicitly agreed to participate in the survey. Likewise, respondents had the option to withdraw from the survey at any moment; exiting the survey or clicking “No” on the informed consent form signature section denoted that participants did not agree to participate.

In this study, the investigator was the only person handling all of the collected information. SurveyMonkey did not supply any PII from registered respondents (SurveyMonkey, 2016). All questions were anonymous and all PII questions in the survey were coded. All survey responses were downloaded to the investigator’s personal computer and deleted from SurveyMonkey and all survey respondents were saved in the investigator’s digital files as numbers. Furthermore, all research data saved to the investigator’s personal computer was password protected and copied to a portable hard drive for use as backup. Hard drives were stored inside a locked file cabinet located in the investigator’s home office; the files will be deleted after 7 years.

Since the six postulated hypotheses were evaluated using SEM, the survey results were processed and examined using SPSS AMOS 25 software. Hypothesis six, which examines the extent to which the predictions of PE were mediated by the PC variable, was also tested using linear regression in SPSS. This statistical software was selected since its drawing and syntax features are user-friendly and it is able to carry out SEM examinations (Kline, 2011). Leedy and Ormrod (2013) indicated that “SEM is a statistical technique to examine the correlations among a number of variables in order to identify possible causal relationships (paths) among the variables” (p. 301). Researchers have considered the SEM statistical procedure, regression analyses, and SPSS AMOS software to be suitable analytical tools, since these have been used in

a number of relevant research projects. For example, Bush et al. (2014) used SEM, linear regression, and Mplus to examine the adoption of “telehealth equipment” (p. 29), Loo et al. (2013) applied a SEM and AMOS analysis to investigate the ergonomic problems influencing the public’s decision in Malaysia to use a countrywide ID card, Addo and Attuquayefio (2014b) used SEM and SPSS AMOS to study “the issues surrounding acceptance of ICT by students of tertiary Institutions” (p. 75), and Al-Abdallah and Al-Qeisi (2014) employed SEM and AMOS to analyze the components of website design influencing users’ use of the system.

Each construct in this investigation was assessed in the survey instrument by three items measured using a five-point Likert scale response format ranging from 1 - Strongly Disagree to 5 - Strongly Agree (see Appendix A). Furthermore, an EFA and a CFA were conducted to examine the underlying relationships in the model, and to assess the fit of the postulated measurement model and causative correlations among independent and dependent variables. According to Leskinen and Niemelä-Nyrhinen (2014), “high correlations between the latent exogenous variables” also known as multicollinearity, is a potential problem that scholars may face when utilizing SEM (p. 3). Therefore, a Pearson correlation coefficient (r) and the tolerance and variance inflation factor (VIF) were used to examine relations between constructs to determine the existence of multicollinearity.

Assumptions

Numerous assumptions were made in the examination of the factors that influence the U.S. public’s acceptance of CBIOSCT. The first assumption was that participants provided honest responses and was derived from their receipt of a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D) along with the questionnaire, explaining the purpose of the study and the safety measures taken to ensure anonymity. A second assumption

was that fear of penalties or privacy violations did not discourage participants from completing the online survey since research subjects understood that their participation was voluntary; they could withdraw from the survey at any moment without consequence and understood the precautionary measures undertaken to maintain privacy.

The third assumption was that the use of CBIOSCT for identity authentication and verification would continue to be an important initiative for the public and private sectors to minimize fraud and enhance protection and privacy. This assumption stemmed from the fact that, in the United States, numerous bills have been introduced in Congress due to concerns about identity crimes. One bill proposed a social security smart card with biometric technology (Social Security Identity Theft Prevention Act, 2008). The Real ID Act (2005) would institute CBIOSCT for drivers' licenses and state ID cards to increase homeland security. Another bill proposed a Medicare smart card with biometric identifiers to minimize fraud and enhance protection and privacy. The Cybersecurity Information Sharing Act (2015) intended to encourage government and businesses to join forces to combat cyber offences and deter identity crimes.

A fourth assumption was that the selected sample truly reflected the opinions of the U.S. public 18 years of age and older, who are legally eligible for a U.S. driver's license or a state identification card and reside in any of the multiple tourist places in the United States. Since the investigation involved 600 randomly selected SurveyMonkey respondents residing in the selected locations, the total number of responses were greater than 88, which was the minimum sample size required for a Chi squared test to attain a true-report probability (Kaelin et al., 2010) and to plausibly approximate the population from which research subjects were selected (Leedy & Ormrod, 2013).

A fifth assumption was that the use of a validated quantitative data collection instrument would produce reliable scores and diminished information bias since other scholars have demonstrated an acceptable reliability of the measure with Taber's (2017) Cronbach's alpha coefficient benchmark of ($0.6 < \alpha < 0.7$). For instance, in Loo et al.'s (2013) measurement model, the coefficient Cronbach's alpha for PE was .80, PC was .75, and intention to use was .71. In another study about the factors influencing patients and healthcare personnel to use telemedicine systems, Bush et al. (2014) reported a reliability coefficient alpha of .865 for SI, .801 for FC, and .941 for BI. Other scholars investigating the factors affecting mobile learning acceptance at a university in Guyana, reported a reliability coefficient alpha of .789 for SI and .797 for FC (Gaffar et al., 2013). For the Attitude factor, Bush et al. (2014) reported a reliability coefficient alpha of .872 and Seyal and Turner (2013) reported a reliability coefficient alpha of .909.

Limitations

Some important limitations on the external and internal validity of the investigation included 1) selection treatment interaction, 2) experimental effects, 3) maturation effects, and 4) sampling bias. The selection treatment interaction limitation involves the generalizability of the results to other demographic segments or groups of individuals (Cottrell & McKenzie, 2011). To mitigate this threat to external validity, a subsection that was representative of the population was cautiously distinguished to conduct the investigation, and research findings were only generalized to the target population. The investigation required that the research sites included residents of the most visited cities by tourists throughout the United States, due to the ease with which incidents of security such as theft, domestic, international, and cross-border terrorism could occur (Mansfeld & Pizam, 2006). Therefore, the target population for the investigation

was reduced substantially and the investigation was delimited to the sample that was representative of the intended population: people residing in New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA. These cities were selected from the importance ranking of U.S. cities most visited by tourists (TripAdvisor, 2016).

The second limitation is the experimental effect, which refers to the different way survey respondents react due to their perception of taking part in an investigation, which in turn threatens both the internal and external validity of research findings (Cottrell & McKenzie, 2011). The third limitation, maturation effects, concerns the change of behavior by survey respondents as a result of diverse issues such as fatigue, stress, and other factors that can happen within a short time interval (Leedy & Ormrod, 2013). Regarding the second limitation, individuals' responses might differ due to their eagerness or fear of being involved in a research study. Conversely, regarding the third limitation, individuals' responses might differ due to their exhaustion or state of mind at the time of taking the survey.

The veracity of the survey and validity of the investigation depended on the participants providing honest answers to survey questions and their willingness to complete the online questionnaire. Levenson (2014) explained that when a survey instrument gathers in-depth demographic data, participants may fear that their answers are not confidential, leading to non-response or untrue responses. Additionally, the alteration of conduct by participants can imperil the internal validity of the research, because the manner in which subjects respond may explain the variations in the dependent variable instead of the independent variables (Leedy & Ormrod, 2013). Likewise, it imperils external validity, because the study findings cannot be generalized since participant responses inadequately reflect the manner that the target population would normally respond (Leedy & Ormrod, 2013).

To address the experimental effects and maturation limitations, SurveyMonkey respondents were provided with a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D) enclosed along with the questionnaire, explaining the purpose of the study and the safety measures taken to ensure anonymity. Moreover, all scales in the measurement instrument were integrated and slightly modified to fit the U.S. context from validated questionnaires that have been demonstrated to be valid and reliable for assessing users' intentions and acceptance in other environments (Bush et al., 2014; Loo et al., 2013; Morosan, 2016). A recent study has demonstrated that U.S. SurveyMonkey panel member responses have a reliability of 85% (Liu & Wronski, 2016). Various scholars have explained that SurveyMonkey panels reach a wide-ranging diverse pool of valid respondents of as many as thirty million people, and that SurveyMonkey conducts benchmarking examinations on a regular basis to make certain that their panel members reflect the characteristics of the U.S. population (Berg et al., 2017, p. 193).

The fourth limitation involves the selection of SurveyMonkey respondents 18 years of age and older, who are legally eligible for a U.S. driver's license or a state identification card, and reside in New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA, which increased the possibility of sampling bias. This form of bias could imperil the internal validity of the investigation, because the manner that subjects were selected and how they responded may explain the variations in the dependent variable instead of the independent variables (Leedy & Ormrod, 2013). Likewise, it could imperil external validity, because the study findings could not be generalized since participants were not a representative sample of the target population (Leedy & Ormrod, 2013). The sampling bias limitation in this investigation was addressed firstly by randomly selecting respondents from SurveyMonkey's

audience. Secondly, the information collected was only generalized to the U.S. public living at tourist destinations throughout the United States. Lastly, due to population and sample boundaries, the information collected was not generalized to members of the U.S. public who are not legally eligible for a Department of Motor Vehicles (DMV) ID card.

Delimitations

An examination of the literature indicated that a strategy being adopted in many countries to detect and deter identity theft and fraud is the implementation of a smart national identity card (SNIC) (Identity Systems, 2017; Loo et al., 2013). However, people's refusal to adopt and use individual authentication technologies is identified as a failure factor in CBIOSC technology implementation (Miltgen et al., 2013). Thus, the scope of this investigation was to provide a further understanding of the issues surrounding the U.S. public's intention to adopt a CBIOSCT in current forms of identification for identity theft and identity fraud prevention in a voluntary setting. Researchers have demonstrated that the UTAUT model is a valuable way to understand acceptance and use of numerous types of technology in various environments and the usage of this model has shown to have satisfactory reliability and validity (Addo & Attuquayefio, 2014b; Hino, 2015; Loo et al., 2013; Miltgen et al., 2013).

Davis et al.'s (2003) UTAUT conceptual framework presents four determinants of individual adoption and usage behavior: "Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), and Facilitating Conditions (FC)" (p. 447). The literature on UTAUT distinguishes different extensions of this framework and stresses the significance of other factors, such as perceived credibility (Loo et al., 2013), privacy, and experience (Hino, 2015). The focus of this investigation, however, was delimited to the application of Loo et al.'s UTAUT model and expanded the model to include attitude (see Figure 1). This delimitation was

made, because to provide a further understanding of the issues surrounding the U.S. public's intention to adopt a CBIOSCT in current forms of identification, it was important to identify the strongest and most significant predictors of the U.S. public's acceptance of CBIOSCT. The UTAUT model applied by Loo et al. (2013) to investigate issues related to Malaysian citizens' approval of SC technology consists of five constructs: PE, PC, SI, FC, and anxiety. In this model, PC and PC were direct determinants of BI, and the prediction of the PE variable was mediated by the PC variable (Loo et al., 2013). Other scholars have studied the effect of attitude on biometric adoption and propose that this construct is also a strong predictor of acceptance and intent to use a technology (Seyal & Turner, 2013).

The variable of anxiety, proposed by Loo et al. (2013), was not included in this investigation, since stress or nervousness does not arise from using CBIOSCT when the technology adoption is voluntary. Also, according to Davis et al. (2003), the anxiety factor has an indirect effect on BI through effort expectancy. The effort expectancy factor was also excluded in this investigation, since using the CBIOSCT requires no time or effort, as participants will only carry the card and present it to legal entities upon request. Thus, the anxiety and effort expectancy factors were judged as not applicable. Furthermore, the investigation was delimited in terms of participants and their geographical location. The study was narrowed to include Americans 18 years of age and older, who are legally eligible for a U.S. driver's license or a state identification card residing in the following areas: New York, NY; Washington, DC; Orlando, FL; Charleston, SC; Las Vegas, NV; and San Francisco, CA.

For the calendar year 2016, the U.S. Census Bureau (2016) estimated that the United States had a total resident population aged 18 years and older of 249,485,228. A recent study revealed that in the United States 15.4 million people were victimized by identity fraud in 2016

(Marchini et al., 2017). This population was outlined to correctly reflect the large U.S. population from which the sample was selected. This investigation required that the research site included residents of the most visited cities by tourists throughout the United States, due to the ease with which incidents of security, such as theft, domestic, international, and cross-border terrorism, could occur (Mansfeld & Pizam, 2006); cities were selected from the importance ranking of U.S. cities most visited by tourists (TripAdvisor, 2016).

Ethical Assurances

Devising, carrying out, and assessing an investigation involves a social trust (Meagher, 2015) that requires ethical behavior from initiation to completion. Therefore, this investigation conformed to all ethical responsibilities delineated in the code of ethics (American Psychological Association, 2010) and the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978). This investigation also fulfilled all other pertinent regulatory and ethical obligations established by NCU's IRB.

Only after obtaining approval from NCU's IRB were questionnaires disseminated and data gathered through SurveyMonkey. Although the measurement instrument of this investigation did not put respondents at risk of harm, as a further step to protect the confidentiality of respondents, the online survey remained anonymous with no names, phone numbers, or emails collected.

Doody and Noonan (2016) explained that some common concerns that may arise prior to beginning an investigation include acquiring necessary authorizations and consent. To address these concerns, site permission from SurveyMonkey was obtained (see Appendix B), and after receiving approval from NCU's IRB, participants were randomly selected and provided with a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D),

explaining the purpose of the study, the safety measures taken to ensure anonymity, the data handling procedures, and clarification that their participation was voluntary. Another ethical concern is coerced participation (American Psychological Association, 2010). To make sure coercion was not a problem in this investigation, no incentives were offered to research respondents. Likewise, research subjects were not menaced or forced to complete the online survey; their participation was voluntary and respondents had the option to withdraw from the survey at any moment without consequences of any kind.

Summary

The aim of this study is to provide a further understanding of the issues surrounding the U.S. public's intention to adopt and use CBIOSCT for identity theft and identity fraud prevention. This chapter covered ten broad areas of the investigation: the research methodology and design, population and sample, measurement instruments, rationalization of how variables were measured, study procedures, the strategies utilized to gather and assess the data, and addressed the assumptions, limitations, delimitations, and ethical considerations. To determine how the public comes to adopt and use this technology, variables from the UTAUT model generated additional insights into the investigation of CBIOSCT acceptance. The data was gathered using an online survey devised to assess the perspectives of the subjects. Six hundred online surveys were distributed through SurveyMonkey among randomly selected SurveyMonkey respondents, after receiving approval from NCU's IRB.

The study survey format was adapted from Loo et al.'s (2013) original questionnaire. All scales in the measurement instrument were integrated and slightly modified to fit the U.S. context from validated questionnaires that have been demonstrated to be suitable and reliable for assessing users' intentions and acceptance in other environments (Bush et al., 2014; Loo et al.,

2013; Morosan, 2016) (see Appendix A). Collected data from SurveyMonkey were used in examining and measuring the extent to which the U.S. public's perceived performance expectancy, perceived credibility, social influence, facilitating condition, and attitude could predict CBIOSCT use intention. Likewise, statistical analyses were conducted to evaluate the extent to which the predictions of PE were mediated by the PC variable. Statistical computations such as AVE, composite reliability, and average loadings were calculated to assess the validity and reliability of the measurement instrument. SEM and SPSS AMOS version 25 software were used to assess the variables under consideration. Hypothesis six, which examines the extent to which the predictions of PE were mediated by the PC variable, was also tested using linear regression in SPSS.

By using a power of 80%, an alpha significance level of .05, and an effect size of .30, with 1 degree of freedom, the *a priori* power analysis estimated a minimum sample size of 88 (see Appendix E). These elements of power calculations were set based on similar studies that have demonstrated an appropriate use of study (Addo & Attuquayefio, 2014b; Al-Abdallah & Al-Qeisi, 2014; Gaffar et al., 2013; Loo et al., 2013). Additionally, an EFA and a CFA were conducted to examine the underlying relationships in the model, and to assess the fit of the postulated measurement model and causal correlations among the independent and dependent variables. A Pearson correlation coefficient (r) and the tolerance and variance inflation factor (VIF) were also used to examine relations between constructs to determine the existence of multicollinearity. In Chapter 4, all results and findings are discussed, and results of the quantitative examinations conducted are used to answer all research questions.

Chapter 4: Findings

The purpose of this nonexperimental correlational quantitative investigation is to determine the extent to which performance expectancy (PE), perceived credibility (PC), social influence (SI), facilitating conditions (FC), and attitude (Att) are predictive of the U.S. public's behavioral intention to use a combined biometric and smart card technology (CBIOSCT), including the extent to which the predictions of PE were mediated by the PC variable. This quantitative study centered on six research questions that were stemmed from the study purpose and the conceptual framework of the UTAUT model, and were examined through online surveys:

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT?

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT?

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT?

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT?

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT?

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility?

The following six null and alternative hypotheses were used to test the six research questions:

H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2₀. Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2_a. Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H6₀. The prediction of performance expectancy is not statistically mediated by perceived credibility.

H6_a. The prediction of performance expectancy is statistically mediated by perceived credibility.

After providing a synopsis of the purpose of the investigation, the discussion of this chapter turns to the investigation's statistical results and evaluation of findings. The statistical results discussion begins with an outline of the questionnaires and information that was gathered. All statistical tests are reported and explained. This is followed by the interpretation of results with reference to the theoretical framework considered in the literature review, questions, and hypotheses of the investigation. The last part of this chapter provides an outline of main points covered.

Validity and Reliability of Data

In this study, research instrument items were adapted from earlier investigations using UTAUT (Loo et al., 2013) and its added components (Bush et al., 2014; Morosan, 2016) to provide a further understanding of the factors influencing the public's acceptance and adoption of novel technologies (see Appendices F–H). G. Sullivan (2011) recommended that researchers use instruments that already exist, since their reliability and validity have been consistently demonstrated in replicated examinations.

During the survey taking process, maturation effects and sampling bias were two important limitations on the external and internal validity of this research study. Maturation effects concern the change of behavior by the survey respondents as a result of diverse issues, such as fatigue, stress, and other factors that can happen within a short time interval (Leedy & Ormrod, 2013). When the study survey was distributed, within the first day of being disseminated, it was stopped automatically by the SurveyMonkey system because of a high rate of abandonment. During the survey process, respondents were provided with the survey

introductory letter (see Appendix C) and the informed consent form (see Appendix D), enclosed along with the questionnaire, explaining the purpose of the study and the safety measures taken to ensure anonymity. Since respondents had to read all these documents before answering the questionnaire, it could be possible that the survey-taking process was perceived as too long, and therefore many participants left before completing it. According to Mol (2017), a low response rate should be anticipated when using a long questionnaire. Individual responses might differ due to exhaustion or state of mind at the time of taking the survey. To address the maturation limitation, the title of the survey and the survey introductory letter were hidden to shorten the survey-taking process without compromising the reliability and validity of the investigation. The approach taken to mitigate the maturation threat resulted in a higher response rate.

Sampling bias was another limitation of the study, because the data gathered in the demographic segment did not account for individuals with annual household incomes between \$150,001 and \$200,000, all other categories of income were considered in the study. Leedy and Ormrod (2013) explained that this form of bias could imperil the internal validity of the investigation, because the manner that subjects were selected and responded may explain the variations in the dependent variable instead of the independent variables. Likewise, it could imperil external validity: the study findings are not generalizable since participants were not a representative sample of the target population (Leedy & Ormrod, 2013). However, this limitation was mitigated as the demographic information was only used to produce a profile of the respondents and not to assess any variations in the study variables. Furthermore, all respondents were randomly selected from SurveyMonkey's audience and the information collected only generalized to the U.S. public living in tourist destinations throughout the United States.

The survey results were processed and examined using SEM and SPSS AMOS version 25 software. The SPSS AMOS statistical software was selected since its drawing and syntax features are user-friendly and allow the researcher to carry out SEM examinations (Kline, 2011). An exploratory factor analysis (EFA) and a confirmatory factor analysis (CFA) were carried out to examine the underlying relationships in the model and to inspect its validity and reliability, as described by Anderson, Babin, Black, and Hair (2014). According to Anderson et al. (2014) a factor loading should be larger than .5 to be considered significant in a factor analysis.

The EFA was conducted using the principal axis factor (PAF) and Promax rotation to reveal the nature of the variables that have an effect on a group of answers (Fidell & Tabachnick, 2014). The Promax rotation outcome is viewed as more correct and reproducible than other rotation methods (Costello & Osborne, 2005). Similarly, the PAF analysis is regarded as more reliable, because it takes measurement errors into consideration without choosing one as the initial communality, it can detect vulnerable factors, and it reveals the factor structure (Kihoro, Ngure, & Waititu, 2015).

The CFA and SEM model, on the other hand, were carried out using the maximum likelihood estimator (MLE). Use of the MLE is common in SEM (Maydeu-Olivares, 2017). Since the MLE of SEM statistical analysis techniques hinges on “multivariate normality assumptions” (Maydeu-Olivares, 2017), all variables used in this investigation were examined for normality using Mardia’s normalized multivariate kurtosis value. In addition, tolerance and the variance inflation factor (VIF) were employed to examine relations between factors to determine the existence of multicollinearity. The absence of multicollinearity issues can be identified by a tolerance value higher than .10 and a VIF value smaller than 10 (Kline, 2011).

Similarly, Bae, He, Lillard, Mayberry, Singh, and Yoo (2014) suggested that a Pearson correlation coefficient larger than .9 is an indication of the presence of substantial collinearity.

Before conducting a factor analysis, the Kaiser-Meyer-Olkin (KMO) index, the Bartlett's test of sphericity, and anti-image correlations were applied to evaluate the suitability of the sample size and data for factor analysis. According to Lackey, Pett, and Sullivan (2003), a factor analysis should not be conducted if the KMO index is less than .6. Likewise, Fidell and Tabachnick (2014) explained that Bartlett's test Chi-square value should be less than .05 of the significance levels for factor analysis to be considered adequate. Then, to test the reliability of the exploratory and confirmatory analyses results, Taber's (2017) Cronbach's alpha coefficient benchmark of ($0.6 < \alpha < 0.7$) was used to show a reasonable internal consistency.

As suggested by Loo et al. (2013), content validity was corroborated through the literature review in this study. Convergent validity was verified by checking that survey items measuring a specific variable loaded distinctly in that variable, by confirming that the average variance extracted (AVE) was higher than .5 (Fidell & Tabachnick, 2014), and by checking that the composite reliability was greater than .7 (Anderson et al., 2014). Finally, discriminant validity was confirmed by verifying that the square root of AVE of each factor was higher than the inter-factor correlation and by checking that the Maximum Shared Variance (MSV) was lower than the AVE value for all factors (Anderson et al., 2014).

Results

Only after obtaining approval from NCU's IRB, the questionnaires were disseminated and data gathered through SurveyMonkey. All participants were provided with a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D), explaining the purpose of the study, the safety measures taken to ensure anonymity, the data handling

procedures, and clarifying that their participation was voluntary. On the informed consent form, participants had the option to provide their names in the signature section and have their names linked to the survey. As explained in the informed consent, any participant information linked to the questionnaire and all data collected have been stored in a safe and secure password protected file and computer that are kept in a locked file cabinet. After 7 years all data will be destroyed. Since SurveyMonkey never makes audience members' PII accessible to anyone, including researchers, the measurement instrument of this investigation did not put respondents at risk of harm, and the confidentiality of respondents remained intact by keeping the online survey anonymous with no names, phone numbers, or emails collected.

The study survey format was adapted from Loo et al.'s (2013) original questionnaire and administered to 100 randomly selected SurveyMonkey audience members residing in each city—New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA—for a total of 600 surveys distributed through SurveyMonkey (see Appendix B). Leedy and Ormrod (2013) indicated that “when the desired sample size is quite large, an online questionnaire is far more cost-effective than a mailed questionnaire” (p. 206). The online survey method utilized in this nonexperimental correlational quantitative investigation enhanced the possibility for each of the participants to respond to questions at their own pace, participate in a low peer-pressure context, skip any question, or end their participation at any time without penalty or prejudgment (Williams, 2012).

Of the 600 online surveys disseminated through SurveyMonkey among randomly selected SurveyMonkey respondents, a total of 333 responses were downloaded from Survey Monkey as an excel file. Then, in the Microsoft Excel spreadsheet program, all data collected was checked for missing values, discrepancies, and errors; 188 of the 333 surveys received were

incomplete and therefore discarded. Seventy-seven of the 188 screened out surveys had fully incomplete responses, in which participants only answered the demographic information section, but did not complete the rest of the questionnaire; 33 participants signed the consent but did not answer the survey, 57 respondents declined participation, and 21 respondents were disengaged, as evidenced by the exact same response being used for every single item. Only 145 participants answered all questions. Since the minimum estimated sample size of 88 was obtained by the power analysis, the amount of completed questionnaires was appropriate for use. By using a power of 80%, an alpha significance level of .05, and an effect size of .30, with 1 degree of freedom, the *a priori* power analysis estimated a minimum sample size of 88 (see Appendix E). These elements of power calculations were set based on similar studies that have demonstrated an appropriate use of study (Addo & Attuquayefio, 2014b; Al-Abdallah & Al-Qeisi, 2014; Gaffar et al., 2013; Loo et al., 2013).

The survey questionnaire in this study included three sections using a nominal and ordinal scale of measurement adapted with permission from Loo et al. (2013). The first section investigated demographic information to produce a profile of the respondents. Demographic questions adapted with permission from Loo et al. (2013) and Morosan (2016) (see Appendices F & G) included age, gender, education level, and annual household income. In addition, the survey data set was processed and examined using SEM and SPSS AMOS version 25 software. The mediation of predictability for the predictor construct of PE by the mediating construct of PC predicting the dependent variable of BI was also tested using linear regression. A regression analysis is appropriate when testing the strength of relationship between constructs (Lewis et al., 2015). The SPSS AMOS statistical software was selected since its drawing and syntax features are user-friendly and allow the researcher to carry out SEM examinations (Kline, 2011).

The demographic information gathered from the study questionnaire included the following: city of current residence, eligibility for a driver's license or a state identification card, gender, age group, highest level of education, and annual household income. In this investigation, the data by city of current residency showed a relatively uniform distribution between Washington, DC (22.10%), Orlando, FL (22.10%), Las Vegas, NV (21.40%), New York, NY (17.20%), and San Francisco, CA (15.20%), except for the low response rate in Charleston, SC (2.10%). A possible reason for this low response rate could be that Charleston, SC is a smaller city in comparison. The tabulation of respondents eligible for a driver's license or a state identification card by gender indicated that participants were predominately female (71.70%), while male participants accounted for 28.30% of the sample. Similarly, participants between 46-63 years (40.70%) and those 64 years old and above (37.90%) comprised the highest percentages of the sample, followed by those aged 25-45 years (17.90%), and 18-24 years (3.40%). To produce a profile of respondents, all demographic characteristics of the study sample were formatted to show their frequency and percentage in Table 1. Appendix J shows all frequency tables, detailing the results of each survey item in the demographic information section.

The second section in the survey assessed PE, PC, SI, FC, and Att. Finally, the third section measured intention to use CBIOSCT in existing forms of personal identification in the United States. Constructs in the last two sections were presented to participants in question form using a five-point Likert scale response format. A summary of items operationalizing all six constructs is presented in Appendix K. The presentation below shows the statistical analysis for each research question with its corresponding hypotheses and survey items.

Table 1.

Demographic Characteristics of the Sample.

Demographic Characteristics	Values	Frequency	Percent (%)
City of current residence	New York, NY	25	17.20
	Washington DC	32	22.10
	Orlando, FL	32	22.10
	Charleston, SC	3	2.10
	Las Vegas, NV	31	21.40
	San Francisco, CA	22	15.20
Legally eligible for a driver's license state ID card	Yes	145	100
Age group	18-24 years old	5	3.40
	25-45 years old	26	17.90
	46-63 years old	59	40.70
	64 years old and above	55	37.90
Gender	Male	41	28.30
	Female	104	71.70
Highest level of education	High school degree or equivalent	27	18.60
	Bachelor of Science/Arts or equivalent	62	42.80
	Master's degree or equivalent	34	23.40
	Doctoral degree or equivalent	10	6.90
	Medical or law degree or equivalent	6	4.10
	Other	6	4.10
Annual household income	\$50,000 or less	48	33.10
	\$50,001 - \$100,000	46	31.70
	\$100,001 - \$150,000	31	21.40
	\$200,001 or more	20	13.80

Note. N=145

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H1₀) and an alternative (H1_a) hypotheses: H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. The PE independent variable was assessed in the survey instrument adapted from

Loo et al. (2013) by three items (PE1, PE2, and PE3) measured using a five-point Likert scale response format (see Table 2).

Table 2.

Performance Expectancy Frequency Table.

PE1. Using CBIOSCT will protect me against identity theft					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	7	4.8	4.8	4.8
	Disagree	9	6.2	6.2	11.0
	Neither agree nor disagree	70	48.3	48.3	59.3
	Agree	53	36.6	36.6	95.9
	Strongly agree	6	4.1	4.1	100.0
	Total	145	100.0	100.0	
PE2. Using CBIOSCT will enhance the reliability of my personal data and thus protect me against identity theft					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	4	2.8	2.8	2.8
	Disagree	12	8.3	8.3	11.0
	Neither agree nor disagree	62	42.8	42.8	53.8
	Agree	57	39.3	39.3	93.1
	Strongly agree	10	6.9	6.9	100.0
	Total	145	100.0	100.0	
PE3. Using CBIOSCT allows for an effective identity verification and authentication process					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	3	2.1	2.1	2.1
	Disagree	6	4.1	4.1	6.2
	Neither agree nor disagree	49	33.8	33.8	40.0
	Agree	76	52.4	52.4	92.4
	Strongly agree	11	7.6	7.6	100.0
	Total	145	100.0	100.0	

Furthermore, **RQ6**. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility? Presented by the following null (H6o) and alternative (H6a) hypotheses: H6o. The prediction of performance expectancy is not statistically mediated by perceived credibility. H6a. The prediction of performance expectancy is statistically mediated by perceived credibility. It was

also measured by the items (PE1, PE2, and PE3) included in the PE scale in the first research question. Table 2 provides a broad impression of how many respondents were located in every single item on the scale of measurement.

Table 3.

Statistical Analysis of Performance Expectancy

	PE1	PE2	PE3	PE Construct
N Valid	145	145	145	145
Missing	0	0	0	0
Mean	3.29	3.39	3.59	3.42
Std. Deviation	0.841	0.844	0.777	0.83
Cronbach's Alpha				0.847
Skewness	-0.663	-0.431	-0.765	-0.44
Kurtosis	1.028	0.535	1.411	0.95

Some important assumptions that underlie the utilization of SEM include: the observations for all measurement scales are unrelated, constructs are unstandardized, data is normally distributed, and the unprocessed data has no missing values (Kline, 2012). Therefore, before conducting the SEM analysis, the raw data was checked for missing values and the sampling distribution of the mean was examined for normality utilizing multivariate kurtosis and skewness values (Kline, 2012). The statistical analysis for the PE construct presented in Table 3, showed no missing values and disclosed that the means for the PE indicators ranged from 3.29 to 3.59, suggesting an overall positive opinion to the items that were measured in the PE variable. The standard deviations for the PE indicators ranged from .777 to .844, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.431 to -.765 and .535 to 1.411 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Moreover, the Cronbach's α score for PE assessed by three items

($\alpha = .847$) showed strong internal reliability with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017).

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H_{20}) and alternative (H_{2a}) hypotheses: H_{20} . Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H_{2a} . Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. The perceived credibility construct was assessed in the survey instrument adapted from Loo et al. (2013) by three items (PC1, PC2, and PC3) measured using a five-point Likert scale response format (see Table 4).

Some important assumptions that underlie the utilization of SEM include: the observations for all measurement scales are unrelated, constructs are unstandardized, data is normally distributed, and the unprocessed data has no missing values (Kline, 2012). Therefore, before conducting the SEM analysis, the raw data was checked for missing values and the sampling distribution of the mean was examined for normality utilizing multivariate kurtosis and skewness values (Kline, 2012). The statistical analysis for the PC construct presented in Table 5, showed no missing values, and disclosed that the means for the PC items ranged from 3.34 to 3.47, suggesting an overall positive opinion to the items that were measured in the PC independent variable. The standard deviations for the PC indicators ranged from .784 to .863, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.079 to -.558 and .255 to .750 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Moreover, the Cronbach's α score for PC assessed by three items

($\alpha = .849$) showed strong internal reliability with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017).

Table 4.

Perceived Credibility Frequency Table.

PC1. CBIOSCT is difficult to be forged by criminals					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	3	2.1	2.1	2.1
	Disagree	11	7.6	7.6	9.7
	Neither agree nor disagree	69	47.6	47.6	57.2
	Agree	46	31.7	31.7	89.0
	Strongly agree	16	11.0	11.0	100.0
	Total	145	100.0	100.0	
PC2. Using CBIOSCT is secure					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	3	2.1	2.1	2.1
	Disagree	11	7.6	7.6	9.7
	Neither agree nor disagree	73	50.3	50.3	60.0
	Agree	50	34.5	34.5	94.5
	Strongly agree	8	5.5	5.5	100.0
	Total	145	100.0	100.0	
PC3. CBIOSCT limits unauthorized access to users' personal information					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	3	2.1	2.1	2.1
	Disagree	10	6.9	6.9	9.0
	Neither agree nor disagree	57	39.3	39.3	48.3
	Agree	66	45.5	45.5	93.8
	Strongly agree	9	6.2	6.2	100.0
	Total	145	100.0	100.0	

Table 5.

Statistical Analysis of Perceived Credibility

	PC1	PC2	PC3	PC Construct
N Valid	145	145	145	145
Missing	0	0	0	0
Mean	3.42	3.34	3.47	3.41
Std. Deviation	0.863	0.784	0.800	0.82
Cronbach's Alpha				0.849
Skewness	-0.079	-0.238	-0.558	-0.19
Kurtosis	0.255	0.708	0.750	1.07

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H3₀) and alternative (H3_a) hypotheses: H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. The SI construct was assessed in the survey instrument adapted from Loo et al. (2013) by three items (SI1, SI2, and SI3) measured using a five-point Likert scale response format. To systematize and simplify the data collected for this question, a frequency distribution table was created. Table 6 provides a broad impression of how many respondents were in every single item on the scale of measurement.

Some important assumptions that underlie the utilization of SEM include: the observations for all measurement scales are unrelated, constructs are unstandardized, data is normally distributed, and the unprocessed data has no missing values (Kline, 2012). Therefore, before conducting the SEM analysis, the raw data was checked for missing values and the sampling distribution of the mean was examined for normality utilizing multivariate kurtosis and skewness values (Kline, 2012). The statistical analysis for the SI construct presented in Table 7 showed no missing values, and disclosed that the means for the SI items ranged from 2.78 to 2.93, suggesting an overall negative opinion to the items that were measured in the SI independent variable. The standard deviations for the SI items ranged from .923 to 1.141, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.089 to .113 and -.100 to -.764 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Moreover, the Cronbach's α score for SI assessed by three

items ($\alpha = .698$) showed a reasonable internal consistency reliability with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017).

Table 6.

Social Influence Frequency Table.

SI1. People who are important to me influence my intention to use CBIOSCT					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	19	13.1	13.1	13.1
	Disagree	31	21.4	21.4	34.5
	Neither agree nor disagree	47	32.4	32.4	66.9
	Agree	37	25.5	25.5	92.4
	Strongly agree	11	7.6	7.6	100.0
	Total	145	100.0	100.0	
SI2. People I know who use CBIOSCT at their workplace influence my intention to use CBIOSCT					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	13	9.0	9.0	9.0
	Disagree	35	24.1	24.1	33.1
	Neither agree nor disagree	68	46.9	46.9	80
	Agree	25	17.2	17.2	97.2
	Strongly agree	4	2.8	2.8	100.0
	Total	145	100.0	100.0	
SI3. The encouragement of U.S. government influences my intention to use CBIOSCT					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	20	18.3	18.3	18.3
	Disagree	33	22.8	22.8	36.6
	Neither agree nor disagree	61	42.1	42.1	78.6
	Agree	21	14.5	14.5	93.1
	Strongly agree	10	6.9	6.9	100.0
	Total	145	100.0	100.0	

Table 7.

Statistical Analysis of Social Influence

	SI1	SI2	SI3	SI Construct
N Valid	145	145	145	145
Missing	0	0	0	0
Mean	2.93	3.91	2.78	2.84
Std. Deviation	1.141	0.923	1.077	1.05
Cronbach's Alpha				0.698
Skewness	-0.091	-0.089	0.113	-0.23
Kurtosis	-0.764	-0.100	-0.356	0.14

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H4₀) and alternative (H4_a) hypotheses: H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. The facilitating conditions construct was assessed in the survey instrument adapted from Loo et al. (2013) by three items (FC1, FC2, and FC3) measured using a five-point Likert scale response format. To systematize and simplify the data collected for this question, a frequency distribution table was created. Table 8 provides a broad impression of how many respondents were in every single item on the scale of measurement.

Some important assumptions that underlie the utilization of SEM include: the observations for all measurement scales are unrelated, constructs are unstandardized, data is normally distributed, and the unprocessed data has no missing values (Kline, 2012). Therefore, before conducting the SEM analysis, the raw data was checked for missing values and the sampling distribution of the mean was examined for normality utilizing multivariate kurtosis and skewness values (Kline, 2012). The statistical analysis for the FC construct presented in Table 9, showed no missing values, and disclosed that the means for the FC items ranged from 3.15 to 3.29, suggesting an overall positive opinion to the items that were measured in the FC independent variable. The standard deviations for the FC indicators ranged from .799 to .981, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.087 to -.415 and -.457 to 1.632 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Moreover, the Cronbach's α score for FC assessed by three

items ($\alpha = .708$) showed satisfactory internal reliability with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017).

Table 8.

Facilitating Conditions Frequency Table

FC1. CBIOSCT infrastructure is available in government and private sectors for identity authentication and fraud risk detection					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	6	4.1	4.1	4.1
	Disagree	10	6.9	6.9	11.0
	Neither agree nor disagree	75	51.7	51.7	62.8
	Agree	46	31.7	31.7	94.5
	Strongly agree	8	5.5	5.5	100.0
	Total	145	100.0	100.0	
FC2. A customer service contact center is available to answer CBIOSCT users' inquiries					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	6	4.1	4.1	4.1
	Disagree	4	2.8	2.8	6.9
	Neither agree nor disagree	86	59.3	59.3	66.2
	Agree	40	27.6	27.6	93.8
	Strongly agree	9	6.2	6.2	100.0
	Total	145	100.0	100.0	
FC3. Current driver's licenses and state ID cards embedded technology are likely to be phased out soon					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	6	4.1	4.1	4.1
	Disagree	31	21.4	21.4	25.5
	Neither agree nor disagree	54	37.2	37.2	62.8
	Agree	43	29.7	29.7	92.4
	Strongly agree	11	7.6	7.6	100.0
	Total	145	100.0	100.0	

Table 9.

Statistical Analysis of Facilitating Conditions

	PE1	PE2	PE3	PE Construct
N Valid	145	145	145	145
Missing	0	0	0	0
Mean	3.28	3.29	3.15	3.24
Std. Deviation	0.837	0.799	0.981	0.88
Cronbach's Alpha				0.708
Skewness	-0.415	-0.322	-0.087	-0.21
Kurtosis	0.931	1.632	-0.457	1.26

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H5₀) and alternative (H5_a) hypotheses: H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. The Attitude construct was assessed in the survey instrument adapted from Bush et al.'s (2014) by three items (Att1, Att2, and Att3) measured using a five-point Likert scale response format. To systematize and simplify the data collected for this question, a frequency distribution table was created. Table 10 provides a broad impression of how many respondents were in every single item on the scale of measurement.

Some important assumptions that underlie the utilization of SEM include: the observations for all measurement scales are unrelated, constructs are unstandardized, data is normally distributed, and the unprocessed data has no missing values (Kline, 2012). Therefore, before conducting the SEM analysis, the raw data was checked for missing values and the sampling distribution of the mean was examined for normality utilizing multivariate kurtosis and skewness values (Kline, 2012). The statistical analysis for the Att construct presented in Table 11 showed no missing values, and disclosed that the means for the Att items ranged from 3.16 to 3.60, suggesting an overall positive opinion to the items that were measured in the Att independent variable. The standard deviations for the Att indicators ranged from .879 to .924, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.441 to -.813 and .485 to .912 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Moreover, the Cronbach's α score for Att assessed by three items

($\alpha = .865$) showed strong internal reliability with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017).

Table 10.

Attitude Frequency Table

Att1. The use of CBIOSCT in existing forms of personal identification in the U.S. to combat identity theft and identity fraud is a good idea					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	6	4.1	4.1	4.1
	Disagree	8	5.5	5.5	9.7
	Neither agree nor disagree	43	29.7	29.7	39.3
	Agree	70	48.3	48.3	87.6
	Strongly agree	18	12.4	12.4	100.0
	Total	145	100.0	100.0	
Att2. I feel that the use of CBIOSCT for identity theft and identity fraud prevention is beneficial					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	5	3.4	3.4	3.4
	Disagree	6	4.1	4.1	7.6
	Neither agree nor disagree	50	34.5	34.5	42.1
	Agree	65	44.8	44.8	86.9
	Strongly agree	19	13.1	13.1	100.0
	Total	145	100.0	100.0	
Att3. The use of CBIOSCT would enhance our standard of living					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	8	5.5	5.5	5.5
	Disagree	16	11.0	11.0	16.6
	Neither agree nor disagree	72	49.7	49.7	66.2
	Agree	43	29.7	29.7	95.9
	Strongly agree	6	4.1	4.1	100.0
	Total	145	100.0	100.0	

Table 11.

Statistical Analysis of Attitude

	PE1	PE2	PE3	PE Construct
N Valid	145	145	145	145
Missing	0	0	0	0
Mean	3.59	3.60	3.16	3.45
Std. Deviation	0.924	0.893	0.879	0.92
Cronbach's Alpha				0.865
Skewness	-0.813	-0.662	-0.441	-0.80
Kurtosis	0.912	0.911	0.485	1.17

Finally, the scale for the dependent variable BI—adapted from Loo et al. (2013)—included three items measuring the extent to which participants in the future will use CBIOSCT for identification purposes and for identity theft and prevention as shown in Table 12.

Table 12.

DV Behavioral Intention Frequency Table.

BI1. I intend to use CBIOSCT for identification purposes					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	8	5.5	5.5	5.5
	Disagree	17	11.7	11.7	17.2
	Neither agree nor disagree	61	42.1	42.1	59.3
	Agree	54	37.2	37.2	96.6
	Strongly agree	5	3.4	3.4	100.0
	Total	145	100.0	100.0	
BI2. I predict I would use CBIOSCT for identity theft and fraud prevention					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	6	4.1	4.1	4.1
	Disagree	17	11.7	11.7	15.9
	Neither agree nor disagree	50	34.5	34.5	50.3
	Agree	64	44.1	44.1	94.5
	Strongly agree	8	5.5	5.5	100.0
	Total	145	100.0	100.0	
BI3. I plan to continue to use CBIOSCT in the future for identity theft and fraud prevention					
		Frequency	%	Valid %	Cumulative %
Valid	Strongly disagree	6	4.1	4.1	4.1
	Disagree	13	9.0	9.0	13.1
	Neither agree nor disagree	79	54.5	54.5	67.6
	Agree	40	27.6	27.6	95.2
	Strongly agree	7	4.8	4.8	100.0
	Total	145	100.0	100.0	

Some important assumptions that underlie the utilization of SEM include: the observations for all measurement scales are unrelated, constructs are unstandardized, data is normally distributed, and the unprocessed data has no missing values (Kline, 2012). Therefore, before conducting the SEM analysis, the raw data was checked for missing values and the

sampling distribution of the mean was examined for normality utilizing multivariate kurtosis and skewness values (Kline, 2012).

The statistical analysis for the BI dependent variable presented in Table 13 showed no missing values, and disclosed that the means for the BI items ranged from 3.20 to 3.35, suggesting an overall positive opinion to the items that were measured in the BI dependent variable. The standard deviations for the BI items ranged from .830 to .909, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.316 to -.646 and .234 to .865 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Moreover, the Cronbach's α score for BI assessed by three items ($\alpha = .900$) showed strong internal reliability with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017).

Table 13.

Statistical Analysis of Behavioral Intention to Use CBIOSCT

	BI1	BI2	BI3	BI Construct
N Valid	145	145	145	145
Missing	0	0	0	0
Mean	3.21	3.35	3.20	3.26
Std. Deviation	0.899	0.909	0.839	0.88
Cronbach's Alpha				0.900
Skewness	-0.611	-0.646	-0.316	-0.48
Kurtosis	0.270	0.234	0.865	0.71

In the above statistical analyses for each research question and dependent variable, results showed that the means for the variables ranged from a low for SI ($M = 2.84$) to a high for Att ($M = 3.45$), suggesting an overall positive opinion to the variables that were measured in the study. PE ($M = 3.42$) was the second most important factor for the U.S. public's BI to use CBIOSCT, followed by PC ($M = 3.41$) and FC ($M = 3.24$). The standard deviations ranged from .82 to 1.05,

suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.19 to -.80 and .14 to 1.26 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014). Similarly, as shown in Table 14, Cronbach's α score indicated that all 18 items assessing the independent and dependent variables showed strong internal reliability with an alpha coefficient of .908.

Table 14.

Summary of Statistical Analysis For All Variables

N = 145	Mean	Standard Deviation	Cronbach's Reliability Coefficient
All Variables	3.27	0.92	0.908

Before conducting a factor analysis, first the research questions and corresponding hypotheses were reiterated. Next, the KMO index, the Bartlett's test of sphericity, and anti-image correlations are applied to evaluate the suitability of the sample size and data for factor analysis. Then, EFA and CFA were conducted to determine the measurement model. Finally, the SEM analysis was carried out to examine the sturdiness of connection among the proposed factors along with a discussion of the results for each of the research questions.

The following six research questions are outlined at the construct level, which in turn, are followed by the relevant null and alternative hypotheses:

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT?

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT?

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT?

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT?

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT?

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility?

The six null and six alternative hypotheses that were utilized to test the six research questions are as follows:

H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2₀. Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2_a. Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H6₀. The prediction of performance expectancy is not statistically mediated by perceived credibility.

H6_a. The prediction of performance expectancy is statistically mediated by perceived credibility.

According to Lackey et al. (2003), the factor analysis should not be conducted if the KMO index is less than .6. Likewise, Fidell and Tabachnick (2014) explained that the Bartlett's test Chi-square value should be less than .05 of the significance levels for factor analysis to be considered adequate. The suitability of the sample size and data for factor analysis are depicted in Table 15. The questionnaire's KMO index of .885 showed that the data set is well suited for factoring. Similarly, the Bartlett's test of sphericity ($X^2(df = 153) = 1605.245, p = 0.000$), indicated that there is significant common variance among the questionnaire items. Additionally, the anti-correlation matrix (see Appendix L) showed all diagonal values greater than .5 (Fidell & Tabachnick, 2014), which indicated a correlation matrix suitable for factor analysis.

Next, an Exploratory Factor Analysis (EFA) was conducted to reveal the nature of the variables that have an effect on a group of answers (Fidell & Tabachnick, 2014). Since the

Promax rotation outcome is regarded as more correct and reproducible than other rotation methods (Costello & Osborne, 2005), the principal axis factor with Promax rotation was selected based on six fixed number of factors to extract and factor loadings higher than .5. Kline (2013) explained that extracting several factors is more beneficial than extracting an insufficient number of factors, to avoid significant errors in the analysis outcome. Furthermore, according to Anderson et al. (2014), a factor loading should be larger than .5 to be considered significant in factor analysis. Items loadings for each factor are shown in Table 15, showing that only five factors (PE, BI, Att, SI, and FC) were underlying the conducted survey. Results in the reproduced correlation table (see appendix M), indicated that there were 2 residuals (1%) with absolute values greater than .05. Kline (2013) suggests that a low residual indicates a high degree of explanatory power of a construct.

Table 15.

Suitability of Sample Size and Data for Factor Analysis

KMO and Bartlett's Test

KMO Measure of Sampling Adequacy		.885
Bartlett's Test of Sphericity	Approx. Chi-Square	1605.245
	df	153
	Sig.	.000

In the analysis, six factors were extracted with eigenvalues of 7.734, 1.928, 1.626, 1.135, .810, and .694, which accounted for 65.69% of the total variance (see Appendix M). Each group of items loaded substantially to one single factor and communalities values ranged from .34 to .96. Costello and Osborne (2005) suggested that communality values ranging from .40 to .70 are considered satisfactory, but values less than .4 may denote additional constructs measured by other items, which could be studied in further investigations. Although SI2 and SI3 exhibited low communalities values, these items were kept for further examination due to their importance

in measuring SI, as highlighted in the literature review section of this study. By using a cut-off of .5 for factor loading, two items FC1 and FC3 were excluded, reducing the items to 16, and excluding the sixth factor, because none of the items loaded higher than .5 to this factor.

Following Anderson et al.'s (2014) recommendations, examination of the scree plot indorsed the retention of five factors as well, because at the sixth factor, the curve begins to flatten out (see Appendix N).

Table 16.

EFA and Communalities

Pattern Matrix ^a						
Constructs Items	Factor					Communalities Extraction
	PE	BI	Att	SI	FC	
PE1	0.69					0.59
PE2	0.81					0.89
PE3	0.70					0.58
PC1	0.94					0.62
PC2	0.78					0.85
PC3	0.66					0.66
SI1				0.92		0.74
SI2				0.56		0.34
SI3				0.57		0.38
FC1						0.59
FC2					0.92	0.72
FC3						0.35
Att1			0.70			0.65
Att2			0.89			0.96
Att3			0.65			0.55
BI1		0.76				0.76
BI2		0.77				0.84
BI3		0.86				0.75

Extraction Method: Principal Axis Factoring.

^a Rotation converged in 7 iterations.

Convergent validity was verified by checking that survey items measuring a specific variable loaded distinctly in that variable, by confirming that the average variance extracted (AVE) was higher than .5 (Fidell & Tabachnick, 2014), and by checking that the composite reliability was greater than .7, as shown in Table 17 (Anderson et al., 2014), except for FC,

which had an AVE value of .41. However, the FC AVE score was considered acceptable, because the composite reliability for this construct was greater than .6, as shown in Table 17 (Fornell & Larcker, 1981).

Table 17.

Convergent Validity, Composite Reliability, and Cronbach's Reliability

Constructs	Number of factor loadings	Average Variance Extracted (AVE)	Composite Reliability	Cronbach's Reliability Coefficient
PE	3	0.54	0.78	0.847
PC	3	0.65	0.84	0.849
SI	3	0.50	0.74	0.698
FC	1	0.41	0.65	0.708
Att	3	0.56	0.79	0.865
BI	3	0.64	0.84	0.900

Cronbach's alpha scores remained the same, indicating high internal reliability with alpha coefficients greater than .70 (Fidell & Tabachnick, 2014). Content validity was corroborated through the literature review in this study. Finally, discriminant validity was confirmed by ensuring survey items did not cross load significantly on other factors and by verifying that the square root of AVE of each factor was higher than the inter-factor correlation as shown in Table 18 (Anderson et al., 2014).

Table 18.

Factor Correlation Matrix and AVE Scores

Factor	AVE	<u>√AVE (in bold)^a and Pearson correlation (non-bold)^b</u>				
		PE	BI	Att	SI	FC
PE	0.54	0.73				
BI	0.64	0.50	0.80			
Att	0.56	0.64	0.69	0.75		
SI	0.50	0.40	0.24	0.24	0.71	
FC	0.41	0.52	0.48	0.53	0.40	0.64

^a Square roots of AVE are shown in bold diagonally.

^b The inter-factor Pearson correlations are shown in non-bold off-diagonally.

After establishing which constructs had an influence on a group of responses, a confirmatory factor analysis (CFA) was then conducted to assess the fit of the parsimonious measurement model and causative correlations among independent and dependent variables (Anderson et al., 2014). According to Leskinen and Niemelä-Nyrhinen (2014), “high correlations between the latent exogenous variables” (p. 3), also known as multicollinearity, is a potential problem that scholars may face when utilizing SEM. Therefore, a Pearson correlation coefficient (r), tolerance and variance inflation factor (VIF) were employed to examine relations between constructs to determine the existence of multicollinearity.

In order to make certain that every construct item was uniformly weighted as a variable in the multicollinearity tests, the values for all items assessing a specific construct were added together and then divided by the number of items measuring that construct to determine an average score. The results of the bivariate correlation method, showed the absolute values of Pearson Correlations among variables lower than .9, which indicated that collinearity issues were less likely to exist (see Appendix O). Bae et al. (2014) suggested that a Pearson correlation coefficient larger than .9 is the indication of the presence of substantial collinearity. The absence of multicollinearity issues can also be identified by a tolerance value higher than .10 and a VIF value smaller than 10 (Kline, 2011). Since all variables had tolerance scores larger than .10 and VIF scores less than 10 (see Appendix O), this outcome pointed to no multicollinearity issues in the study.

Confirmatory Factor Analysis and SEM

The CFA and SEM model were carried out using the MLE. Use of the MLE is common in SEM (Maydeu-Olivares, 2017). Since MLE of SEM statistical analysis techniques hinge on “multivariate normality assumptions” (Maydeu-Olivares, 2017), all variables used in this

investigation were examined for normality utilizing Mardia's normalized multivariate kurtosis value. As shown in Table 19, Mardia coefficients of the dependent and independent variables in this study were lower than their critical ratios, denoting high data normality.

Table 19.

Assessment of Normality

Variable	Mardia's Kurtosis Value	Critical Ratio
FC3	-0.48	-1.19
FC2	1.54	3.77
SI3	-0.39	-0.95
SI2	-0.14	-0.34
SI1	-0.78	-0.34
Att3	0.43	1.05
Att2	0.84	2.06
Att1	0.84	2.06
BI3	0.79	1.95
BI2	0.19	0.46
BI1	0.22	0.54
PC3	0.68	1.68
PC2	0.64	1.58
PC1	0.21	0.51
PE3	1.32	3.25
PE2	0.48	1.17
PE1	0.95	2.34
Multivariate	113.18	26.81

To determine a good fit of the parsimonious measurement model in the EFA analysis and to evaluate the SEM model, the following five indexes were considered in the confirmatory factor analysis: a ratio of Chi-square to degrees of freedom (χ^2/df) less than 2, a Comparative Fit Index (CFI) score greater than .95, a Root Mean Square Error of Approximation (RMSEA) value less than .08, a Tucker Lewis Index (TLI) higher than .95, and a Normed Fit Index (NFI) of at least .9 (Anderson et al., 2014; Howard, 2013). Results showed that the EFA measurement model exhibited a poor goodness-of-fit (the ratio of $\chi^2/df = 2.136$, $p < .001$; CFI = .907; RMSEA = .089; TLI = .887; NFI = .842).

A customary way to improve the fit of a model in SEM is to check the model modification indices for any proposed correlations between the construct's items residual errors (Hermida, 2015). However, an important reliability assumption underlying the utilization of SEM is that the exogenous variables are measured free of error (Kline, 2012). Violating this assumption could lead to bias, which will prejudice the path estimates for exogenous variables and the outcome of the study findings (Kline, 2012). Furthermore, correlating measurement errors to enhance model fit may also affect the path estimate and hence disguise the true model (Hermida, 2015). According to Brown (2015), correlation of errors should not occur with the exclusive objective of enhancing model fit, instead it should be performed substantiated based on past studies or theoretical concepts.

In the CFA, the measurement instrument signpost a poor fit. However, the model obtained in the EFA, in which the properties, validity, reliability, and statistical significance of the measurement instrument of this study had been examined, showed a satisfactory output. After confirming that the configuration of modeled relationships was estipulated as intended, modification indices (MIs) and residuals were then examined to continue assessing the adequacy of the measurement instrument. MIs calculate approximately the anticipated variation in the structural model Chi-square if a parameter constrained to zero is unconstrained (Kline, 2011). Since model fit can also be affected by the wording of the items on the scale of measurement (Brown, 2015), the arrangement of each survey item was examined. MIs and residuals pointed out to add error covariance between the PE factor's items, and to correlate errors between the SI factor's indicators. The suggested correlations in MIs may reflect an item of answer approaches linked with the wording of the indicators that are closely connected perceptually (Brown, 2015).

After modifying the model based on MIs by adding covariances between the construct's items residual errors (Breckler, 1990), a satisfactory model fit was attained (the ratio of $\chi^2/df = 1.490$, $p < .001$; CFI = .964; RMSEA = .058; TLI = .954; NFI = .900). For the PE factor, the MI pointed to the covariance between the residual errors for the following items: “using CBIOSCT will enhance the reliability of my personal data, thus protecting me against identity fraud” (PE2) and “using CBIOSCT allows for an effective identity verification and authentication process” (PE3). For PC, the MI suggested covarying the following PC items residual errors: “CBIOSCT is difficult to be forged by criminals” (PC1) and “using CBIOSCT is secure” (PC2).

Finally, for SI the MI indicated adding a covariance among residual errors for its three measurement items: “people who are important to me influence my intention to use CBIOSCT” (SI1), “people I know who are using CBIOSCT at their workplace influence my intention to use CBIOSCT” (SI2), and “the encouragement of the U.S. government influences my intention to use CBIOSCT” (SI3). Since these measures are worded similarly, a non-zero covariance between the residual errors for the above-mentioned items is plausible (Ahn, Jin, & Myers, 2011). In the CFA original model, FC1 loaded to the SI factor and not the FC factor as expected; thus, it was removed. Deleting FC1 from the analysis ensured a good fit between the model and the data. Figures 2 and 3 explain the modified measurement model with standardized and non-standardized estimates respectively, extracted after adding covariances and FC1 removal.

Convergent validity of the measurement model was verified by confirming that the AVE value was higher than .5 (Fidell & Tabachnick, 2014) and by checking that the composite reliability was greater than .7, as shown in Table 20 (Anderson et al., 2014), except for FC, which had an AVE value of .44. However, the FC AVE score was considered acceptable,

because the composite reliability for this construct was greater than .6, as shown in Table 20 (Fornell & Larcker, 1981). These results revealed a high concordance with the EFA outcome.

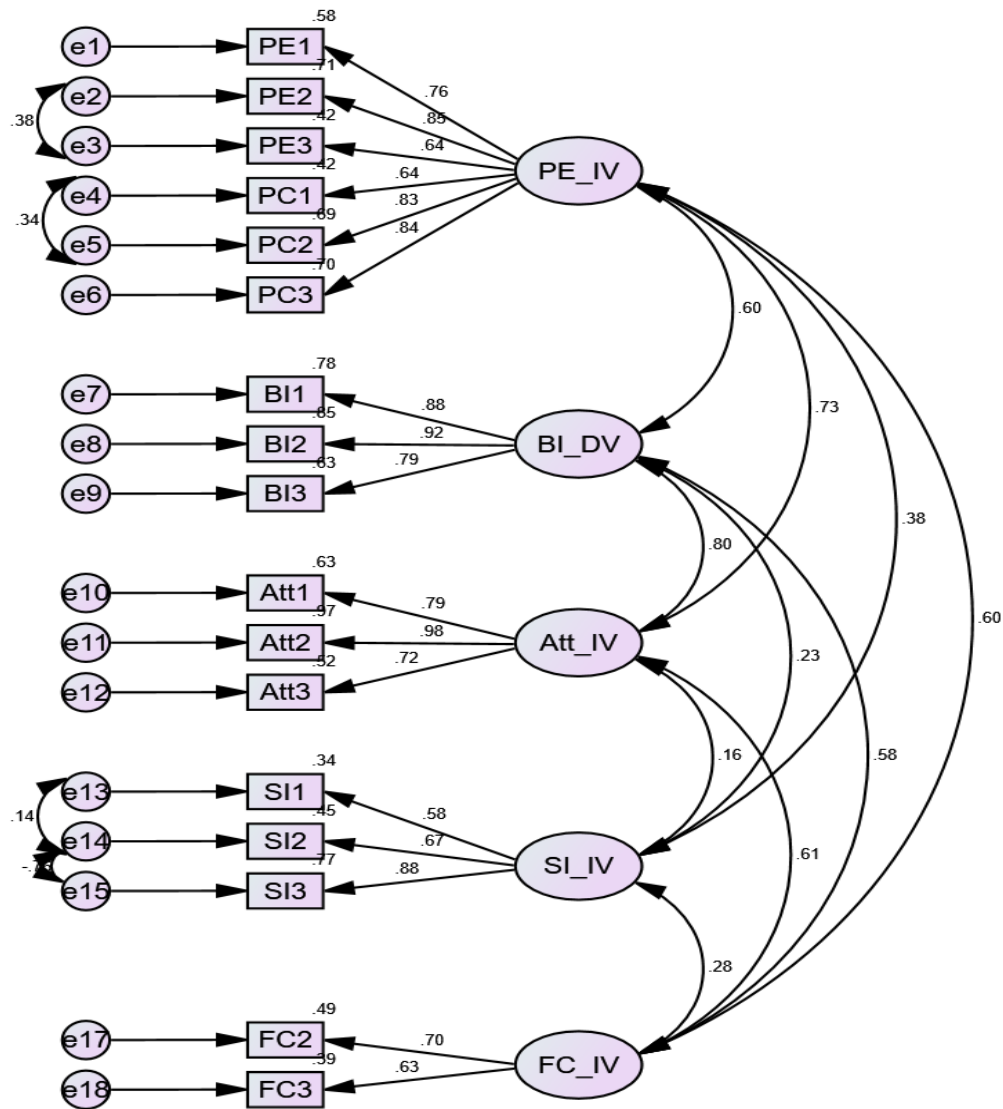


Figure 2. Measurement model: Factor loadings, covariance between the residual errors, latent variable covariances, R-square values, and standardized path estimates.

Note. Tests of model fit using maximum likelihood (ML) estimation (N = 145): The ratio of χ^2/df = 1.490, $p < .001$; CFI = .964; RMSEA = .058; TLI = .954; NFI = .900.

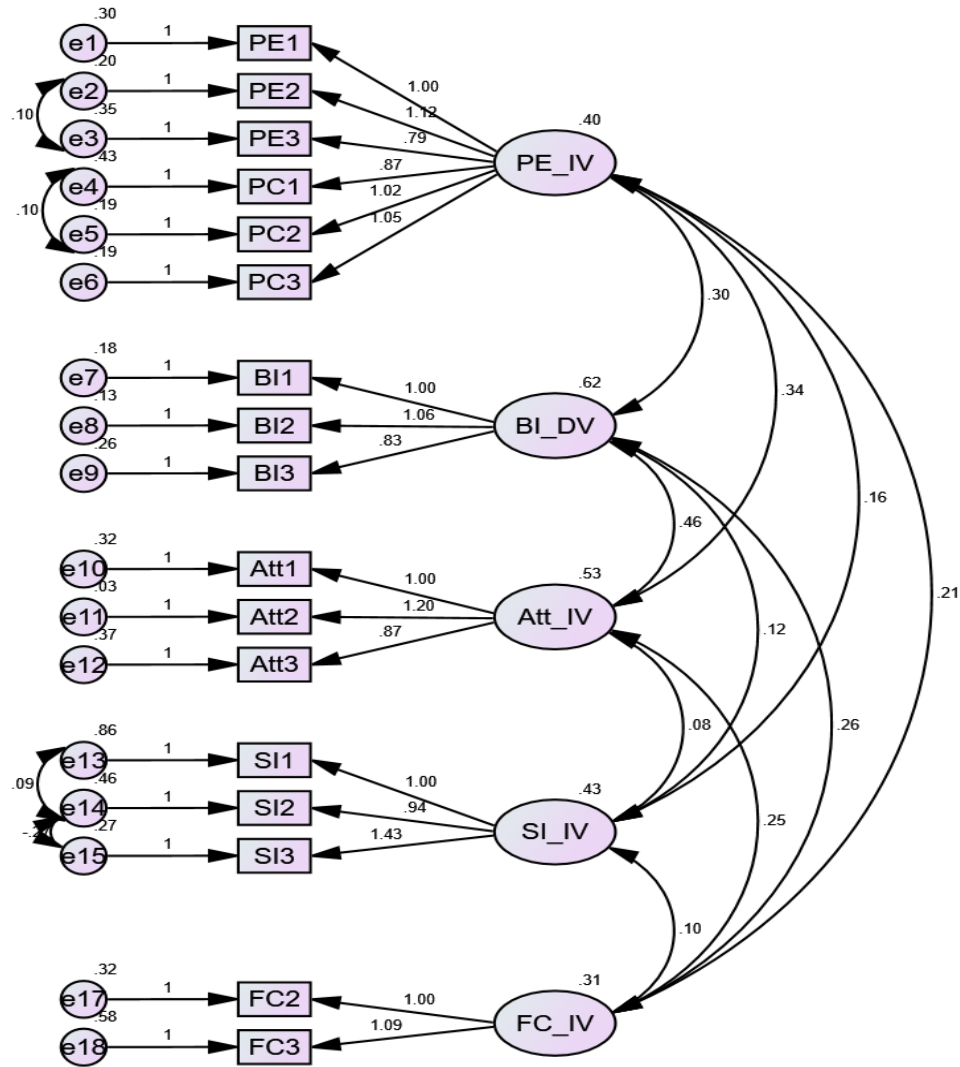


Figure 3. Measurement model: Factor loadings, covariance between the residual errors, latent variable covariances, R-square values, and unstandardized path estimates.

Note. PE_IV = Performance Expectancy Independent Variable; BI_DV = Behavioral Intention Dependent Variable; Att_IV = Attitude Independent Variable; SI_IV = Social Influence Independent Variable; FC_IV = Facilitating Conditions Independent Variable.

Tests of model fit using maximum likelihood (ML) estimation (N = 145): The ratio of $\chi^2/df = 1.490$, $p < .001$; CFI = .964; RMSEA = .058; TLI = .954; NFI = .900.

Table 20.

Measurement of Model Reliability and Validity

Factor	N	AVE	CR	MSV	Cronbach's Reliability Coefficient	$\sqrt{\text{AVE}}$ (in bold) ^a and Pearson correlation (non-bold) ^b				
						SI	PE	BI	Att	FC
SI	3	0.52	0.76	0.14	0.635	0.72				
PE	3	0.59	0.89	0.53	0.847	0.38	0.76			
BI	3	0.75	0.90	0.64	0.900	0.23	0.60	0.87		
Att	3	0.70	0.88	0.64	0.865	0.16	0.73	0.80	0.84	
FC	2	0.44	0.61	0.37	0.602	0.28	0.60	0.58	0.61	0.67

Note. N: Number of factor loadings, CR: Composite Reliability, MSV: Maximum Shared Variance

^a Square roots of Average Variance Extracted (AVE) are shown in bold diagonally.

^b The inter-factor Pearson correlations are shown in non-bold off-diagonally.

Since FC1 was removed in the analysis, Cronbach's alpha scores decrease for FC, as shown in Table 20. The Cronbach's α score for the FC factor ($\alpha = .67$) assessed by two items showed a reasonable internal consistency reliability, with an alpha coefficient greater than the acceptable suggested benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017). For the other constructs, Cronbach's alpha scores remained the same, indicating high internal reliability, with alpha coefficients greater than .70 (Vogt, 2007). Similarly, the intercorrelations among constructs presented in Table 20 showed the absolute values of Pearson Correlations among variables lower than .9, which indicated that collinearity issues were less likely to exist (Bae et al., 2014). These results revealed a high concordance with the EFA outcome. Content validity was corroborated through the literature review in this study. Finally, discriminant validity was confirmed by verifying that the square root of AVE of each factor was higher than the inter-factor correlation and by checking that the Maximum Shared Variance (MSV) was lower than the AVE value for all factors, as shown in Table 20 (Anderson et al., 2014).

SEM Parsimonious Model and Results

After establishing the measurement model through the CFA, SEM assumptions of multicollinearity were reexamined. The tolerance and variance inflation factor (VIF) were employed to examine relations between factors to determine the existence of multicollinearity. The absence of multicollinearity issues can be identified by a tolerance value higher than .10 and a VIF value smaller than 10 (Kline, 2011). Since all variables had tolerance scores larger than .10 and VIF scores less than 10 (see Appendix P), this outcome pointed to no multicollinearity issues in the study.

As the measurement model presented evidence of reliability and validity in the CFA, a path analysis for the SEM parsimonious model was carried out (Anderson et al., 2014) to test hypotheses formulated in the conceptual research framework. Findings of the SEM parsimonious model PE, SI, FC, Att, and BI exhibited satisfactory fit indices (ratio of $\chi^2/df = 1.333$, $p < .001$; CFI = .989; RMSEA = .048; TLI = .982; NFI = .959). The overall results of hypotheses testing are shown in Table 21, and Figure 4 depicts a parsimonious model with an unstandardized path coefficient and the coefficient of determination (R^2) value. Findings of the SEM parsimonious model indicated that the extended UTAUT model explained a high percentage (73%) of the variance for BI to use CBIOSCT ($R^2 = 0.73$).

Table 21.

Summary of Hypothesis Testing

Hypotheses	Path	Remarks
H1 ₀ .	PE is not a predictor of BI	Supported
H1 _a .	PE is a predictor of BI	Not supported
H2 ₀ .	PC is not a predictor of BI	Supported
H2 _a .	PC is a predictor of BI	Not supported
H3 ₀ .	SI is not a predictor of BI	Supported
H3 _a .	SI is a predictor of BI	Not supported
H4 ₀ .	FC is not a predictor of BI	Not supported
H4 _a .	FC is a predictor of BI	Supported
H5 ₀ .	Att is not a predictor of BI	Not supported
H5 _a .	Att is a predictor of BI	Supported
H6 ₀ .	PE is not mediated by PC	Not supported
H6 _a .	PE is mediated by PC	Supported

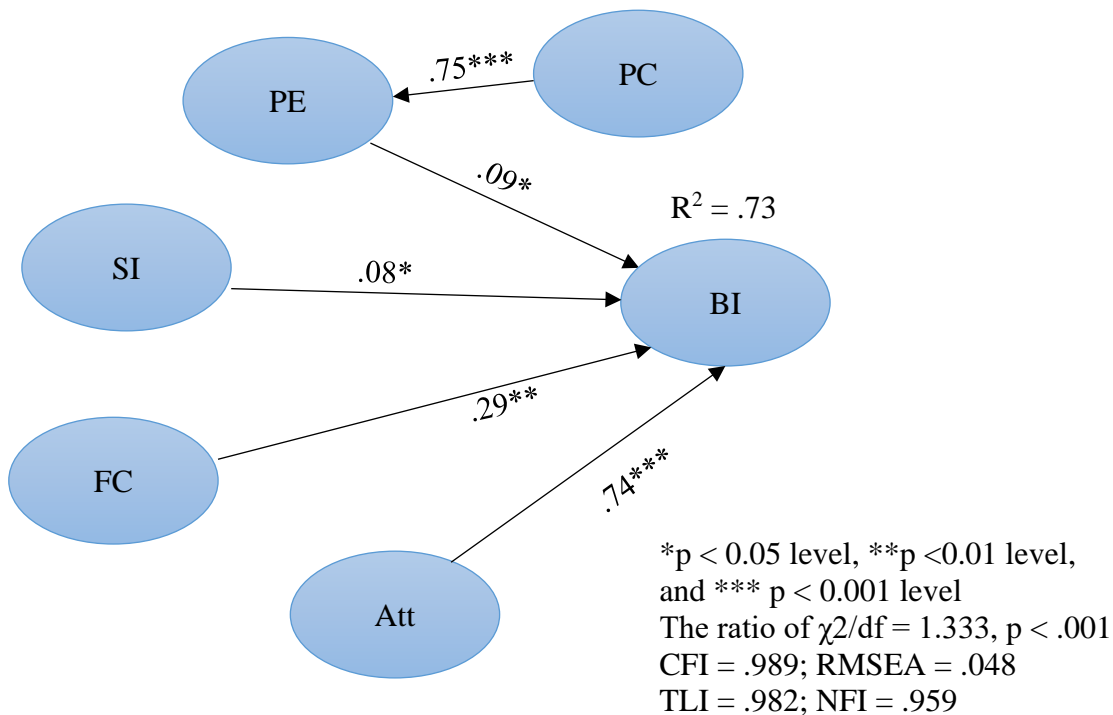


Figure 4. Research parsimonious model: R-square values, and unstandardized path estimates.

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT? This question was evaluated by testing its null and alternative hypotheses. As shown in Table 22, the findings of this investigation revealed that the alternative hypothesis (H1_a), which anticipated that PE would be a statistically significant predictor of the U.S. public's BI to use CBIOSCT, was not supported ($\beta = .073$, $p < .05$). Thus, the null hypothesis (H1_o) that anticipated that PE would not be a statistically significant predictor of the U.S. public's BI to use CBIOSCT was supported.

Table 22.

Test of Performance Expectancy Effects

Path	Path Coefficient	Standard Error	Beta	C.R.	p value
PE predictor of BI	0.09	0.06	0.073	1.564	0.118 ^a

^a Not significant at the .05 level.

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT? After testing this question's null and alternative hypotheses, the findings of this analysis also rejected alternative hypothesis (H2_a), which predicted that PC is a statistically significant predictor of the U.S. public's BI to use CBIOSCT. The second hypothesis (H2) revealed that PC did not explain any variance of the BI factor, and therefore was extracted as a mediator of PE and not as a predictor of BI, as shown in Figure 4. Hence, the null hypothesis (H2_o), which forecasts that PC is not a statistically significant predictor of the U.S. public's BI to use CBIOSCT, was supported.

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT? As shown in Table 23, the analysis of this question's null and alternative hypotheses found that there is no significant relationship between SI and BI ($\beta =$

.064, $p < .05$). Thus, the null hypothesis (H3₀), that SI is not a statistically significant predictor of the U.S. public's BI to use CBIOSCT, was supported.

Table 23.

Test of Social Influence Effects

Path	Path Coefficient	Standard Error	Beta	C.R.	p value
SI predictor of BI	0.08	0.06	0.064	1.352	0.176 ^a

^a Not significant at the .05 level.

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT? This question was evaluated by testing its null and alternative hypotheses. As shown in Table 24, the findings of this investigation showed that FC positively affects BI ($\beta = .179$, $p < .01$). Hence the alternative hypothesis (H4_a), that FC is a statistically significant predictor of the U.S. public's BI to use CBIOSCT, is supported and the null hypothesis is rejected.

Table 24.

Test of Facilitating Conditions Effects

Path	Path Coefficient	Standard Error	Beta	C.R.	p value
FC predictor of BI	0.29	0.11	0.179	2.648	0.008 ^a

^a Significant at the .01 level.

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT? The analysis of this question found that the alternative hypothesis (H5_a), that anticipated that Att would be a statistically significant predictor of the U.S. public's BI to use CBIOSCT, was supported ($\beta = .701$, $p < .001$). Consequently, the null hypothesis (H5₀), that Att was not a statistically significant predictor of the U.S. public's BI to use CBIOSCT, was rejected.

Table 25.

Test of Attitude Effects

Path	Path Coefficient	Standard Error	Beta	C.R.	p value
Att predictor of BI	0.74	0.07	0.701	10.931	**a

^a Significant at the .001 level.

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility? This question's null and alternative hypotheses were tested utilizing SEM and linear regression. As shown in Table 26, the findings of this investigation revealed that PC serves as an inter-mediator variable in explaining the variances of PE ($\beta = .75$, $p < .001$). Thus, the alternative hypothesis (H6_a) that predicts that PE is statistically mediated by PC is supported and the null hypothesis (H6₀) is rejected.

Table 26.

Performance Expectancy Mediating Effects by Perceived Credibility

	Path	Path Coefficient	Std. Error	Beta	C.R.	p value
SEM Analysis	PE mediated by PC1	0.90	0.12	0.67	7.869	**a
	PE mediated by PC2	1.00	0.10	0.82	9.587	**a
	PE mediated by PC3	1.02	0.11	.82	9.654	**a
Linear Regression	PE mediated by PC	0.75	0.06	0.75 ^b	13.574 ^c	**a

^a Significant at the .001 level.

^b Standardized regression coefficient from linear regression.

^c T-statistics coefficient.

Evaluation of Findings

The aim of this investigation was to provide a further understanding of the issues surrounding the U.S. public's intention to adopt and use CBIOSCT for identity theft and identity fraud prevention. To determine the factors that shape the U.S. public's acceptance of CBIOSCT, the investigation framework used Loo et al.'s (2013) extension of UTAUT to include PE, PC, SI,

and FC constructs, and expanded the model to include Att. The effect of each independent variable on the U.S. public's BI to utilize CBIOSCT was examined, and the extent to which the predictions of the variable PE were mediated by the construct of PC was also explored. The results of the study found theoretical and empirical support for the competence of the UTAUT framework to provide a better understanding of the factors influencing user acceptance of biometrics (BIO) and smart card (SC) technologies. What follows explains the findings of each of the research questions (RQ) addressed in this investigation.

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H1₀) and alternative (H1_a) hypotheses: H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

Interestingly, in answering this research question, it was found that PE did not affect BI. In other words, the PE factor did not explain any variance of BI. Thus, the NULL was accepted. This finding indicates that the U.S. public does not believe that using CBIOSCT will limit their chances of becoming the target of identity bandits, and therefore it does not influence their intention to use it. This result contradicts previous investigations that observed a significant relationship between the PE and BI factors (Hino, 2015; Loo et al., 2013; Mtebe & Raisamo, 2014). However, this finding supports the assertion of Loo et al. (2013) that the Malaysian public does not perceive the use of a countrywide smart ID card to be an effective mechanism to deter criminal acts. The underlying principle for these contradictions might lie in the fact that

these investigations (Hino, 2015; Loo et al., 2013; Mtebe & Raisamo, 2014) examined other attributes in dissimilar settings.

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H2₀) and alternative (H2_a) hypotheses: H2₀. Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H2_a. Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

Based on the SEM analysis results, the null hypothesis was accepted, because PC did not explain any variance of the BI factor. This finding indicates that the security and confidentiality of a system does not influence the U.S. public intention to use it. This result is inconsistent with Loo et al. (2013) and Hino (2015). A possible theoretical reason is that, with the wide variety of advanced technologies and schemes used by criminals to steal people's PII (Clough, 2015), the public perceives identity theft as a challenging behavior to tackle (Hsieh et al., 2012). Therefore, people might see PC as an irrelevant factor for their intention to use the technology.

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H3₀) and alternative (H3_a) hypotheses: H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

The findings of H3 showed that there was no significant effect of SI on BI; thus, the NULL hypothesis was accepted. This result supports the NULL hypothesis assessment that the U.S. public's intention to use CBIOSCT is not influenced by the views and motivations of someone who holds a meaningful position in their lives. This outcome concurs with Davis et

al.'s (2003) findings, which suggested that SI is not a significant predictor of intention to use technology when the adoption of technology is voluntary. Other scholars that have examined the effect of SI on BI in different voluntary settings also reported similar results (AlGhamdi, Alshehri, & Drew, 2012).

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H4₀) and alternative (H4_a) hypotheses: H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

Results in the SEM analysis found a positive effect of FC on the U.S. public's intention to use CBIOSCT, and thus the null hypothesis was rejected and the alternative accepted. This outcome suggests that an adequate specialized, administrative, and technological structure must exist to facilitate acceptance and use of CBIOSCT. This result supports previous findings reported in other investigations (Addo & Attuquayefio, 2014b; Ali et al., 2016; Gaffar et al., 2013).

The significant correlation between FC and Att (see Appendix Q) also indicates that public attitudes towards the use of CBIOSCT pivot around the existence of adequate infrastructure (FC factor). Although this relationship was not postulated in the conceptual research framework of the study, this finding is consistent with those produced by Dwivedi et al. (2014). However, it is in contrast with Bilgihan, Khalilzadeh, and Ozturk (2017), who argued that FC does not have any effect on Att and BI, and suggested security as a positive factor influencing user attitude towards the use of a system.

Another study about the acceptance of mobile electronic medicals record found a significant impact of PE on Att (Hwang et al., 2016). The rationale for these contrasts might lie in the fact that these investigations were conducted in different contexts examining other features. Bilgihan et al. (2017) and Hwang et al. (2016) studied the adoption of systems that have other technological capabilities and mobile accessibility, whereas this investigation examined the adoption of a combined biometric smart card technology that will only serve as form of identity verification.

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H5₀) and alternative (H5_a) hypotheses: H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

The overall results of hypotheses testing revealed that Att was the strongest predictor of the U.S. public's intention to use CBIOSCT, and thus the null hypothesis was rejected and the alternative accepted. This indicates that the U.S. public's positive or negative attitude toward CBIOSCT will be the key to their adoption and intention to use it. This supports Seyal and Turner's (2013) findings that users' attitudes about BIO significantly predict the acceptance and intention to use a technology. Likewise, this finding concurs with Gaffar et al. (2013), who suggested that Att is the strongest determinant of BI.

To enhance the likelihood of acceptance and use of CBIOSCT, the U.S. public and private sectors need to have a general understanding of the issues surrounding the U.S. public's intention to adopt CBIOSCT in current forms of identification for identity theft and fraud

prevention. Based on the results of this investigation, the U.S. public will exhibit a positive attitude towards the use of CBIOSCT when they believe that the appropriate infrastructure exists.

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility? This question presented the following null (H_{60}) and alternative (H_{6a}) hypotheses: H_{60} . The prediction of performance expectancy is not statistically mediated by perceived credibility. H_{6a} . The prediction of performance expectancy is statistically mediated by perceived credibility.

Even though PC was not a significant predictor of BI, in the SEM analysis PC was found as an inter-mediator variable in explaining the changes of the performance expectancy factor, thus, supporting the alternative hypothesis H_{6a} . This outcome is analogous to results reported by Loo et al. (2013), who observed a positive relationship between PC and PE. This result is also consistent with the findings of H1 and H2. Since identity theft is a challenging behavior to tackle (Hsieh et al., 2012), it is feasible that the U.S. public does not perceive a CBIOSCT as an advantageous system to dissuade identity crimes, and therefore PE and PC do not have a positive impact on BI.

Summary

The study survey format was adapted from Loo et al.'s (2013) original questionnaire and the research instrument items were adapted from instruments developed by Loo et al. (2013), Bush et al. (2014), and Morosan (2016). The study survey was distributed through Survey Monkey, among Survey Monkey respondents. Of the 333 responses downloaded from Survey Monkey, only 145 participants answered all questions. However, the minimum estimated sample size, obtained by the power analysis, was 88, and therefore the amount of completed questionnaires was appropriate for use.

To determine the factors that shape the U.S. public's acceptance of CBIOSCT, the investigation framework used Loo et al.'s (2013) extension of UTAUT to include PE, PC, SI, and FC as independent variables, and expanded the model to include Att as another independent variable. The survey results first were processed and examined using SEM and SPSS AMOS version 25 software, with principal axis factor (PAF) as the method for parameter estimation in the exploratory factor analysis.

The data by city of current residency showed a relatively uniform distribution between Washington, D.C. (22.10%), Orlando, FL (22.10%), Las Vegas, NV (21.40%), New York, NY (17.20%), and San Francisco, CA (15.20%), except for the low response rate in Charleston, SC (2.10%). The tabulation of respondents eligible for a driver's license or a state identification card by gender indicated that participants were predominately female (71.70%), while males accounted for 28.30%. The statistical analysis for all constructs presented showed that the standard deviations ranged from .82 to 1.05, suggesting a fairly narrow spread of values around the mean. Examination of the skewness and kurtosis values, which ranged from -.19 to -.80 and .14 to 1.26 respectively, indicated that the data was univariate normal, because indices were within the acceptable range between -2 and +2 (Gravetter & Wallnau, 2014).

The EFA analysis showed that only five factors (PE, BI, Att, SI, and FC) were underlying the conducted survey. After assessing the presence of possible collinearity issues and checking the validity and reliability of the EFA parsimonious measurement model, a CFA was conducted to assess model fit. The CFA and the SEM model were carried out utilizing the maximum likelihood estimator. Results showed that the EFA measurement model exhibited a poor goodness-of-fit (the ratio of $\chi^2/df = 2.136$, $p < .001$; CFI = .907; RMSEA = .089; TLI = .887;

NFI = .842). After establishing the measurement model through the CFA, SEM assumptions of multicollinearity were reexamined and the validity and reliability of the model were confirmed.

The SEM parsimonious model found that PE, SI, FC, Att, and BI exhibited satisfactory fit indices (The ratio of $\chi^2/df = 1.333$, $p < .001$; CFI = .989; RMSEA = .048; TLI = .982; NFI = .959). Results of the first research question found that PE did not affect BI. This finding indicates that the U.S. public does not believe that using CBIOSCT will limit their chances of becoming the target of identity bandits, and therefore it does not influence their intention to use it. Results of the second research question revealed that PC did not explain any variance of the BI factor, and thus was not extracted as an influential factor in the SEM analysis. The findings of the third research question showed that there was no significant effect of SI on BI. This result supports the assessment that the U.S. public's intention to use CBIOSCT is not influenced by the views and motivations of someone who holds a meaningful position in their lives.

On the other hand, results of the fourth research question disclosed a positive effect of FC on the U.S. public's intention to use CBIOSCT. This outcome suggests that an adequate specialized, administrative, and technological structure must exist to facilitate acceptance and use of CBIOSCT. The finding of the fifth research question revealed that Att was the strongest predictor of the U.S. public's intention to use CBIOSCT. This indicates that the U.S. public positive or negative attitudes toward CBIOSCT will be the key to their adoption and intention to use it. Finally, the result of the sixth research question found PC as an inter-mediator variable in explaining the changes of the PE factor. Findings of the SEM parsimonious model indicated that the extended UTAUT model explained a high percentage (73%) of the variance for behavioral intention to use CBIOSCT ($R^2 = 0.73$). Contributions, limitations, and possible future research on the subject are discussed in detail in Chapter 5.

Chapter 5: Implications, Recommendations, and Conclusions

This chapter presents a synopsis of the study, its limitations, and ethical considerations. It continues with a discussion of its findings and the implications for user authentication technology adoption practices, education, and research. Finally, the discussion turns to the recommendations and conclusions, with thoughts on future investigations and for ongoing technology adoption education that stemmed from this research.

The problem investigated in this study was the factors associated with the acceptability of combined biometric and smart card technology (CBIOSCT) in current forms of identification for identity theft and fraud prevention. The escalation of identity theft and fraud has become a major source of concern for the public and U.S. law enforcement agencies (Cassim, 2015). A strategy adopted in many countries to detect and deter identity theft and fraud is the implementation of a smart national identity card (SNIC) (Identity Systems, 2017; Loo et al., 2013). However, the refusal to adopt and use individual authentication technologies is identified as a failure factor in CBIOSCT implementation (Miltgen et al., 2013).

To determine the factors that shape the U.S. public's acceptance of CBIOSCT, the investigation framework used Loo et al.'s (2013) extension of Davis et al.'s (2003) UTAUT model, which posits that performance expectancy (PE) is mediated by perceived credibility (PC), and suggests PE, PC, social influence (SI), and facilitating conditions (FC) as contributing factors of technology acceptance and adoption. This model was expanded to include attitude (Att) as another determining factor. Davis et al. (2003) suggested that when PE and effort expectancy are excluded from the UTAUT framework, the effect of Att should be considered. In this investigation, the effort expectancy factor was omitted since CBIOSCT is very simple to use: the cardholder shows an ID at the agencies' request. Hence, Att was incorporated instead.

This investigation used a nonexperimental, correlational, quantitative approach, because constructs were assessed in their original form with no manipulation (Cano et al., 2014). The purpose of this investigation was to examine the relationship between the independent variables of PE, PC, SI, FC, and Att on the dependent variable of the U.S. public's behavioral intention (BI) to use CBIOSCT. This study also evaluated the extent to which the predictions of PE were mediated by the PC variable. This quantitative study centered on six research questions stemming from the study purpose and the conceptual framework of the UTAUT model, and examined through online surveys:

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT?

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT?

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT?

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT?

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT?

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility?

The following six null and alternative hypotheses were used to test the six research questions:

H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2₀. Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H2_a. Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

H6₀. The prediction of performance expectancy is not statistically mediated by perceived credibility.

H6_a. The prediction of performance expectancy is statistically mediated by perceived credibility.

The data were gathered using an online survey devised to assess the perspectives of the subjects. Using an online survey tool and panel was the best choice, because it is the most robust and prominent tool in scholarly investigations (Balasubramanian et al., 2017; Elbeck, 2014). Furthermore, the online survey enhanced the possibility for each of the participants to respond to questions at their own pace, participate in a low peer-pressure context, skip any question, or end their participation at any time without penalty or prejudgment (Williams, 2012).

The study survey format was adapted from Loo et al.'s (2013) original questionnaire and research instrument items were adapted with permission from instruments developed by Loo et al. (2013), Bush et al. (2014), and Morosan (2016). Both the research instrument items and survey were modified to fit the investigation context (see Appendix A). G. Sullivan (2011) recommended that researchers use instruments that already exist since their reliability and validity have been consistently demonstrated in replicated examinations.

The investigation online questionnaire was administered to 100 randomly selected SurveyMonkey audience members residing in each city— New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA— for a total of 600 surveys. Of the 600 online surveys disseminated, a total of 333 responses were downloaded from Survey Monkey. In the Microsoft Excel spreadsheet program, all data collected was checked for missing values, discrepancies, and errors; 188 surveys were discarded. Only 145 participants answered all questions; however, since the minimum estimated sample size obtained by the power analysis was 88, the amount of completed questionnaires was appropriate for use (see Appendix E).

In this investigation, all results were tested using the SEM technique and SPSS AMOS software. The mediation of predictability for the predictor construct of PE by the mediating construct of PC on the DV BI was also tested using linear regression. A regression analysis is appropriate when testing the strength of relationship between constructs (Lewis et al., 2015). Furthermore, an exploratory factor analysis (EFA) and a confirmatory factor analysis (CFA) were conducted to examine the underlying relationships in the model, and to assess the fit of the postulated measurement model and causative correlations among independent and dependent variables. The SPSS AMOS statistical software was selected since its drawing and syntax features are user-friendly and allows the researcher to carry out SEM examinations (Kline, 2011).

Limitations

Some important limitations on the external and internal validity of the investigation included 1) selection treatment interaction, 2) experimental effects, 3) maturation effects, and 4) sampling bias. The selection treatment interaction limitation involves the generalizability of the results to other demographic segments or groups of individuals (Cottrell & McKenzie, 2011). To mitigate this threat to external validity, a subsection that was representative of the population was cautiously distinguished to conduct the investigation, and research findings were only generalized to the target population. The investigation required that the research site included residents of the most visited cities by tourists throughout the United States, due to the ease with which incidents of security such as theft, domestic, international, and cross-border terrorism could occur (Mansfeld & Pizam, 2006). Therefore, the target population for the investigation was reduced substantially and the investigation was delimited to the sample that was representative of the intended population: people residing in New York, NY; Washington, DC;

Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA. These cities were selected from the importance ranking of U.S. cities most visited by tourists (TripAdvisor, 2016).

The second limitation, experimental effects, refers to the different way survey respondents react due to their perception of taking part in an investigation, which in turn threatens both the internal and external validity of research findings (Cottrell & McKenzie, 2011). The third limitation, maturation effects, concerns the change of behavior by the survey respondents as a result of diverse issues such as fatigue, stress, and other factors that can happen within a short time interval (Leedy & Ormrod, 2013). In the second limitation, individuals' responses might differ due to their eagerness or fear of being involved in a research study. Conversely, in the third limitation, individuals' responses might differ due to their exhaustion or state of mind at the time of taking the survey.

The veracity of the survey and validity of the investigation depended on the participants providing honest answers to survey questions and on their willingness to complete the online questionnaire. Levenson (2014) explained that when a survey instrument gathers in-depth demographic data, participants may fear that their answers may not be confidential, leading to non-response or false responses. Additionally, the alteration of conduct by the participants of an investigation can imperil the internal validity of the research, because the manner that subjects responded may explain the variations in the DV instead of the IVs (Leedy & Ormrod, 2013). Likewise, it imperils external validity, because the study findings cannot be generalized since participants' responses inadequately reflect the manner that the target population would normally respond (Leedy & Ormrod, 2013).

To address the experimental effects and maturation limitations, SurveyMonkey respondents were provided with a survey introductory letter (see Appendix C) and an informed

consent form (see Appendix D) enclosed along with the questionnaire, explaining the purpose of the study and the safety measures taken to ensure anonymity. Moreover, all scales in the measurement instrument were integrated and slightly modified to fit the U.S. context from validated questionnaires that have been demonstrated to be valid and reliable for assessing users' intentions and acceptance in other environments (Bush et al., 2014; Loo et al., 2013; Morosan, 2016). A recent study demonstrated that U.S. SurveyMonkey panel member responses have a reliability of 85% (Liu & Wronski, 2016). Various scholars have explained that SurveyMonkey panels reach wide-ranging diverse valid respondents of as many as thirty million people, and have pointed out that SurveyMonkey conducts benchmarking examinations on a regular basis to make certain that their panel members reflect the characteristics of the U.S. population (Berg et al., 2017, p. 193).

During the survey taking process, maturation effects were an important limitation on the external and internal validity of this research study. When the study survey was distributed, it was stopped automatically by the SurveyMonkey system because of a high rate of abandonment. During the survey process, respondents were provided with the survey introductory letter (see Appendix C), and the informed consent form (see Appendix D) enclosed along with the questionnaire, explaining the purpose of the study and the safety measures taken to ensure anonymity. According to Mol (2017), low response rate should be anticipated when utilizing a long questionnaire. To address this limitation, the title of the survey and the survey introductory letter were hidden to shorten the questionnaire without compromising the reliability and validity of the investigation. The approach taken to mitigate the maturation threat result in a higher response rate.

For the fourth limitation, the selection of SurveyMonkey respondents 18 years of age and older, who are legally eligible for a U.S. driver's license or a state identification card, and reside in New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA, increased the possibility of sampling bias. In addition, during the survey taking process, sampling bias was an important limitation on the external and internal validity of this research study, because the data gathered in the demographic segment did not account for individuals with an annual household income between \$150,001 and \$200,000. These forms of bias could imperil the internal validity of the investigation, because the manner that subjects were selected and responded may explicate the variations in the dependent variable instead of the independent variables (Leedy & Ormrod, 2013). Likewise, it could imperil the external validity, because the study findings could not be generalized since participants were not a representative sample of the target population (Leedy & Ormrod, 2013).

Sampling bias limitations in this investigation were addressed firstly by randomly selecting respondents from SurveyMonkey's audience. Secondly, the information collected was only generalized to the U.S. public living at tourist destinations throughout the United States. Thirdly, due to population and sample boundaries, the information collected was not generalized to members of the U.S. public who are not legally eligible for a Department of Motor Vehicles (DMV) identification (ID) card. Lastly, the demographic information was only used to produce a profile of the respondents and not to assess any variations in the study variables.

Only after obtaining approval from the NCU's IRB, the questionnaires were disseminated and data gathered through SurveyMonkey. All participants were provided with a survey introductory letter (see Appendix C) and an informed consent form (see Appendix D), explaining the purpose of the study, the safety measures taken to ensure anonymity, the data handling

procedures, and clarifying that their participation was voluntary. In the informed consent, participants had the option to provide their names in the signature section and have their names linked to the survey. As explained in the informed consent, the agreed participants' information linked to the questionnaire and all data collected have been stored in a safe and secure password protected file and computer that are kept in a locked file cabinet. After 7 years all data will be destroyed. Since SurveyMonkey never makes audience members' PII accessible to anyone, including researchers. The measurement instrument of this investigation did not put respondents at risk of harm, the confidentiality of respondents remained intact by keeping the online survey anonymous with no names, phone numbers, or emails collected.

Implications

The use of smart cards and biometric systems is a concept that has been described and evaluated in numerous ways, including concerns about privacy in the workplace (Carpenter et al., 2016), uses for crime deterrence (Pocs, 2013), responses to user perception and behavior (Loo et al., 2013), and benefits as an effective component of a countrywide ID system (Benjamin et al., 2014). Furthermore, the extant investigations on the topic have concentrated on either user perceptions toward biometric technology (Harinda & Ntagwirumugara, 2015; Miltgen et al., 2013; Morosan, 2016), or both smart card (SC) and biometric (BIO) technology in mandatory settings (Fahl et al., 2013; Loo et al., 2013). However, there has been little analytical work done on the issues surrounding the adoption of CBIOSCT in current forms of ID in the U.S. for identity theft and fraud prevention in voluntary settings. Therefore, the focus of this investigation was on providing a further understanding of the factors affecting the U.S. public's BI to adopt CBIOSCT. Understanding the determinants associated with the acceptability of BIO and SC technologies for combating identity theft and fraud in the U.S. would be able to lead private

and public organizations to devise and implement sound strategies, policies, and procedures that will warrant effective implementation and vast adoption of a combined biometric smart card (CBIOSC) ID.

The study findings have important theoretical and practical implications. From a theoretical standpoint, empirical evidence of this study revealed that the UTAUT model is suitable for studying the determinants of CBIOSC adoption and use, as the extended UTAUT model used in this research accounted for 73% of the variance in BI to use CBIOSC. From a practical viewpoint, the results of this study offer scholars and practitioners important insight into comprehending the U.S. public's acceptance of CBIOSC, potentially accelerating the improvement of current forms of identification, which, in turn, could be a valuable instrument to assist in combating identity theft and identity fraud in the United States.

Ever since the establishment of the UTAUT model, researchers have demonstrated that it is a valuable way to establish the factors that influence individuals to adopt new technologies, such as information and communication technology (ICT) (Addo & Attuquayefio, 2014b), mobile electronic medical records (Hwang et al., 2016), e-learning technologies (Shaqrah, 2015), biometric technology (Harby et al., 2012), and SC applications (Chong et al., 2011). In this investigation, the variables examined in the expanded UTAUT framework presented a satisfactory level of reliability and validity throughout the investigation, as indices were within the acceptable range: Cronbach's alpha coefficient benchmark of ($0.6 < \alpha < 0.7$) (Taber, 2017); AVE higher than .5 (Fidell & Tabachnick, 2014); composite reliability greater than .7 (Anderson et al., 2014); a ratio of Chi-square to degrees of freedom (X^2/df) less than 2; a CFI score greater than .95; a RMSEA value less than .08; a TLI higher than .95; and a NFI of at least .9 (Anderson et al., 2014; Howard, 2013). Hence, this investigation adds empirical evidence to the literature

by studying the competence and soundness of the UTAUT framework, which was formed in a workplace setting (Davis et al., 2003), to explicate the U.S. public's intentions to use CBIOSCT in a voluntary context at multiple tourist destinations throughout the U.S.

This study concentrated on six research questions devised to explore respondents' perceptions of UTAUT factors associated with the acceptability of CBIOSCT in current forms of ID for combating identity theft and fraud. Research findings draw attention to three key issues: (1) enabling components should exist to encourage acceptance of CBIOSCT, (2) improving the U.S. public's attitudes would increase people's intentions to adopt CBIOSCT, and (3) enhancing the U.S. public's perception of security, robustness, and reliability of CBIOSCT requires the promotion of the recognition of CBIOSCT's benefits, thus boosting adoption of the technology in current forms of ID to deter identity theft and fraud. What follows explains the findings and implications of each research question.

RQ1. To what extent, if any, does the performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H1₀) and alternative (H1_a) hypotheses: H1₀. Performance expectancy is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H1_a. Performance expectancy is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

Interestingly, this study found that PE did not affect BI. In other words, the PE factor did not explain any variance in BI. Thus, the null hypothesis (H1₀) was accepted. This finding indicates that the U.S. public does not believe that using CBIOSCT will limit their chances of becoming the target of identity bandits, and therefore it does not influence their intention to use it. This result contradicts previous investigations that observed a significant relationship

between the OE and the BI factors (Hino, 2015; Loo et al., 2013; Mtebe & Raisamo, 2014). However, this finding supports the assertion of Loo et al. (2013) that the Malaysian public does not perceive the use of a countrywide smart ID card to be an effective mechanism to deter criminal acts. The underlying principle for these contradictions might lie in the fact that these investigations examined other attributes in dissimilar settings.

This result can be seen as significant to the detection and election of the correct technology-based determinant factor for CBIOSCT acceptance. Even though prior research has identified PE as an important predictor of BI (Brenčić et al., 2016; Davis et al., 2003; Hino, 2015; Loo et al., 2013), the non-significant relationship found between PE and BI in this study may explain that CBIOSCT in current forms of ID is not perceived as an advantageous mechanism to deter ID theft and fraud and, consequently, it is not a predictor of intention to use it. A possible reason could be that identity theft and fraud problems are so prevalent and widespread in the U.S. (ITRC, 2017) that the U.S. public may perceive that the use of CBIOSCT may not protect them against these type of identity crimes.

RQ2. To what extent, if any, does the perceived credibility predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H2₀) and alternative (H2_a) hypotheses: H2₀. Perceived credibility is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H2_a. Perceived credibility is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

Based on the SEM analysis results, the null hypothesis was accepted because PC was not attributed to explain any variance of the BI factor. This finding indicates that the security and confidentiality of a system does not influence the U.S. public intention to use it. This result is inconsistent with Loo et al. (2013) and Hino (2015). A possible theoretical reason is that with

the wide variety of advanced technologies and schemes used by criminals to steal people's PII (Clough, 2015), the public perceives identity theft as a challenging behavior to tackle (Hsieh et al., 2012); therefore, people might see PC as an irrelevant factor to their intention to use.

RQ3. To what extent, if any, does the social influence predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H3₀) and alternative (H3_a) hypotheses: H3₀. Social influence is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H3_a. Social influence is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

The findings of H3 showed that there was no significant effect of SI on BI, and thus the null hypothesis was accepted. This result supports the assessment that the U.S. public's intention to use CBIOSCT is not influenced by the views and motivations of someone who holds a meaningful position in their lives. This outcome concurs with Davis et al.'s (2003) findings, which suggested that SI is not a significant predictor of intention to use technology when the adoption is voluntary. Other scholars that have examined the effect of SI on BI in different voluntary settings also reported similar results (AlGhamdi et al., 2012; Kim, Lee, & Wang, 2017).

RQ4. To what extent, if any, do the facilitating conditions predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H4₀) and alternative (H4_a) hypotheses: H4₀. Facilitating conditions are not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H4_a. Facilitating conditions are a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

Results in the SEM analysis found a positive effect of FC on the U.S. public's intention to use CBIOSCT, and thus the null hypothesis was rejected and the alternative accepted. This

outcome suggests that an adequate specialized, administrative, and technological structure must exist to facilitate acceptance and use of CBIOSCT. This result supports previous findings reported in other investigations (Addo & Attuquayefio, 2014b; Ali et al., 2016; Gaffar et al., 2013).

The significant correlation between FC and Att (see Appendix Q) also indicates that the public's attitudes towards the use of CBIOSCT pivot around the existence of adequate infrastructure (FC factor). Although this relationship was not postulated in the conceptual research framework of the study, this finding is consistent with those produced by Dwivedi et al. (2014). However, it is in contrast with Bilgihan et al. (2017), who argued that FC does not have any effect on Att and BI, and suggested security as a positive factor influencing user attitude towards the use of a system.

Another study about the acceptance of mobile electronic medical record found a significant impact of PE on Att (Hwang et al., 2016). The rationale for these contrasts might lie in the fact that these investigations were conducted in different contexts examining other features. Bilgihan et al. (2017) and Hwang et al. (2016) studied the adoption of systems that have other technological capabilities and mobile accessibility, whereas this investigation examined the adoption of a combined biometric smart card technology that will only serve as a form of identity verification.

RQ5. To what extent, if any, does attitude(s) predict the U.S. public's behavioral intention to use CBIOSCT? This question presented the following null (H5₀) and alternative (H5_a) hypotheses: H5₀. Attitude(s) is not a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT. H5_a. Attitude(s) is a statistically significant predictor of the U.S. public's behavioral intention to use CBIOSCT.

The overall results of hypotheses testing revealed that Att was the strongest predictor of the U.S. public's intention to use CBIOSCT, and thus the null hypothesis was rejected and the alternative accepted. This indicates that the U.S. public's positive or negative attitudes toward CBIOSCT will be the key to their adoption and intention to use it. This supports the assertion made by Seyal and Turner (2013) that users' attitude about BIO significantly predicts the acceptance and intention to use the technology. Likewise, this finding concurs with Gaffar et al. (2013), who suggested Att to be the strongest determinant of BI. To enhance the likelihood of acceptance and utilization of CBIOSCT, the U.S. public and private sectors need to have a general understanding of the issues surrounding the U.S. public's intention to adopt CBIOSCT in current forms of identification for identity theft and identity fraud prevention. Based on the results of this investigation, the U.S. public will exhibit a positive attitude toward using CBIOSCT when they believe that the appropriate infrastructure exists.

RQ6. To what extent, if any, does performance expectancy predict the U.S. public's behavioral intention to use CBIOSCT when accounting for perceived credibility? This question presented the following null (H6₀) and alternative (H6_a) hypotheses: H6₀. The prediction of performance expectancy is not statistically mediated by perceived credibility. H6_a. The prediction of performance expectancy is statistically mediated by perceived credibility.

Even though PC was not a significant predictor of BI, in the SEM analysis, PC was found to be an inter-mediator variable in explaining the changes of the PE factor, thus supporting the alternative hypotheses H6_a. This outcome is analogous to results reported by Loo et al. (2013), who observed a positive relationship between PC and PE. This result is also consistent with H1 and H2 findings. Since identity theft is a challenging behavior to tackle (Hsieh et al., 2012), it is

feasible that the U.S. public does not perceive a CBIOSCT as an advantageous system to dissuade identity crimes, and therefore PE and PC do not have a positive impact on BI.

Investigations in the area of BIO and SC technology adoption have been limited in comparison to the acceptance of other technological innovations (Loo et al., 2013; Seyal & Turner, 2013). Findings in the extended version of UTAUT used in this study imply that FC and Att are direct determinants of BI and that the predictions of the PE variable are mediated by the PC variable. Findings of this investigation may also indicate that the U.S. public residing at tourist destinations may be less influenced by other individuals' recommendations or views, but more influenced by their own perceptions of the availability of adequate CBIOSCT infrastructure in the public and private sectors for identity authentication and fraud risk detection, thus leading to a more positive attitude towards the adoption and use of technology. Finally, the study results may suggest that raising awareness of CBIOSCT's safety and privacy features, objectives, infrastructure, and support may help the U.S. public realize the benefits of implementing this technology and how it can help to combat identity crimes.

This investigation adds to the understanding of why individuals adopt technology, which can help develop better systems for devising, constructing, and implementing CBIOSCT in a way that will increase the chances of user acceptance. Furthermore, comprehending the factors that influence the U.S. public's acceptance of CBIOSCT in current forms of identification for identity theft and fraud prevention would provide insights that might enable lawmakers, organizations, financial institutions, and identity management service providers to offer an appropriate identity authentication and verification solution, create a high-perceived value for citizens, and minimize the costs and incidence of identity crimes.

Recommendations for Practice

The rate of identity theft and fraud is remarkably rising every day (ITRC, 2017), affecting societies around the world, and lamentably, it is not a problem that will end anytime soon (Cassim, 2015). In an effort to combat identity crimes and make societies safer, governments around the globe are embracing authentication mechanisms with CBIOSCTs (Agbaraji et al., 2014). Various scholars are confident that a convergence of BIO and SC technologies can effectively authenticate and verify the identity of an individual (Das et al., 2014; Karuppiah & Saravanan, 2014; Li, Lu, X. Yang, & Y. Yang, 2015), but, so far, there is limited research of the factors associated with the adoption of these technologies.

Different scholars that have examined the public's adoption and willingness to use a technology have confirmed the appropriateness and validity of the UTAUT model in predicting BI in different settings across a wide variety of technologies (Bytha et al., 2014; Dowd et al., 2015; Weng et al., 2012). Additionally, scholars have argued that UTAUT offers a sturdy theoretical base for exploring user technology adoption and use, and that in order to provide a more thorough comprehension of IT acceptance, UTAUT needs to be expanded (Bytha et al., 2014; Chauhan & Jaiswal, 2016; Gunawardena & Samaradiwakara, 2014). The findings of this investigation further support these assertions, since the extended UTAUT model used in this research accounted for 73% of the variance in BI to use CBIOSCT.

The results of this study offer scholars and practitioners important insights into understanding the U.S. public's perspectives of CBIOSCT at multiple tourist destinations throughout the United States. Comprehending the factors influencing user acceptance of CBIOSCT in current forms of identification for identity theft and fraud prevention would enable lawmakers, organizations, financial institutions, and identity management service providers to

devise suitable future provisions and policy measures to tackle the challenges identity theft crimes pose. According to the findings of this research, both FC and Att have a positive impact on the intention of CBIOSCT use. It seems that the biometric smart card infrastructure and the U.S. public's attitude in the adoption of CBIOSCT are two important constraints for the satisfactory implementation of an identity authentication and verification solution for identity theft and fraud prevention.

The positive relationship between perceived FC and BI to use a technology found in this study has been supported by various investigations highlighting its importance for explaining the acceptance of IT innovations (Addo & Attuquayefio, 2014b; Ali et al., 2016; Gaffar et al., 2013). Hence, FC issues, such as the availability of CBIOSCT infrastructure in the U.S.'s public and private sectors for identity authentication and fraud risk detection (FC1), a customer service contact center in case of any questions relating to the CBIOSCT (FC2), and the expectation that current driver's licenses and state ID cards are likely to be phased out soon (FC3), should be addressed. It is recommended that the government and any institution that requires identity verification of individuals should spend more on biometric and smart card infrastructure set up, maintenance, and updates. In addition, these organizations should provide an online and phone hotline to address questions and concerns relating to CBIOSCT implemented in existing forms of personal identification. In these circumstances, increasing people's adoption of CBIOSCT in current forms of ID in the United States is likely.

The strong influence of attitude on BI to use a technology found in this study has also been supported by numerous studies underscoring the importance of this driver in predicting the adoption of novel systems (Gaffar et al., 2013; Hwang et al., 2016; Seyal & Turner, 2013). The significant correlation between FC and Att observed in this investigation also indicates that the

public's attitudes toward the use of CBIOSCT pivot around the existence of adequate infrastructure. Therefore, Att issues, such as the extent to which participants perceive that using CBIOSCT is a good idea (Att1), is beneficial (Att2), and will enhance their standard of living (Att3), should be addressed. It is recommended that the government and any corporation that requires identity verification of individuals should raise awareness regarding CBIOSCT objectives, features, impact, available resources, and advantages through the dissemination of this information to the public. Equipping the public with the pertinent information and resources will lead to a more positive attitude toward the technology, which may translate into adoption of CBIOSCT in current forms of ID in the United States.

In this research, PC was also found as an inter-mediator variable in explaining the predictions of BI, as measured by the PE determinant. This outcome is analogous to results reported by Loo et al. (2013), who observed a positive relationship between PC and PE. PC consist of the following issues: the extent to which CBIOSCT is perceived as being difficult to forge (PC1), secure (PC2), and limiting unauthorized access to users' personal information (PC3). PE, on the other hand, concerns the extent to which the U.S. public believes that using CBIOSCT will protect them against identity theft (PE1), enhance the reliability of their personal data, thus protecting them against identity fraud (PE2), and allow for an effective identity verification and authentication process (PE3). Thus, developers should take into consideration PC and PE issues in addressing CBIOSCT acceptability.

Since the study findings also suggest that the U.S. public does not perceive a CBIOSCT as a robust and reliable system to deter the challenging behavior of identity theft and fraud (Hsieh et al., 2012), and therefore PE and PC don't have a positive impact on BI. It is recommended that the public and private sectors should devise and enforce tailor-made policies

and measures for validating and confirming the cardholder's identity, for safeguarding the cardholder's information, and for alerting inconsistencies in the cardholder's authentication process. Yücel (2013) indicated that the establishment of red flag guidelines can be a valuable tool for organizations, since these rules operate as an "early warning system" to uncover and deter fraud (p. 154). The FTC Identity Theft Rules (2007) also instructs creditors and business in the financial sector to frequently evaluate the suitability of current validation and safeguarding methods and keep them up-to-date as new vulnerabilities emerge.

In the United States, Congress enacted the Real ID ACT of 2005, to thwart extremists and felons from obtaining identification documents, such as driver's licenses and state ID cards (Martin et al., 2015). Another aim of this legislation was to enhance the trustworthiness, soundness, and precision of identification cards issued by the states (Martin et al., 2015). To prevent disapproval of the legislation, supporters of the enhanced state-issued ID cards avowed that the Real ID Act would be indispensable in thwarting illegal immigrants, averting terror attack plots, and diminishing ID fraud (Real ID Act proceedings and debates, 2005). This law was enacted in response to the terrorist acts of September 11, 2001, in which attackers used fake papers and valid state-issued ID cards to move freely throughout the United States without raising concern or suspicion (Miller, 2016). However, critics of the Real ID Act claim that the benefits of this legislation are minimal compared to the high danger for identity theft victimization, since criminals could potentially breach the DMVs' systems and plunder databases (Kravitz, 2009; Thiessen, 2008).

A similar technology used throughout the government by federal employees and contractors is Smart Card (SC). All DoD employees, contractors, and soldiers are required to use a Common Access Card (CAC) in order to access physical, logical, and network DoD resources

(DoD, 2014). The ID card issued by the federal government to its personnel is capable of verifying and confirming the cardholder's identity, storing information about the user, authenticating, recording, and tracing the user's operations, and verifying ID holders' privileges to authorize their physical and logical access to systems and data (Draper et al., 2012). CAC technology provides a more rigorous way to confirm and validate the cardholder's identity as it is used in conjunction with a personal identification number (PIN), public key infrastructure (PKI) authentication tools, personal identity verification (PIV) certificates, and biometric technology (DoD, 2014).

Li et al., (2015) suggested that combined SC and biometric (BIO) technology can provide strong verification and validation of the cardholder's identity. Therefore, it is recommended that the government implement CBIOSCT in existing forms of personal identification, beyond required federal government agencies to the general public, private, and commercial sectors and nongovernmental organizations. Additionally, the government should advertise to the general public that CBIOSCT in existing forms of personal identification will provide robust data security, validated and verified access, and sturdy protection against exploitation, alteration, and forgery (Li et al., 2015b). The U.S. public should also be informed of who will gain access to the information stored in the ID using CBIOSCT, which agency will be in charge of keeping the ID card holder's information up-to-date, and what type of data will be accessed during the identity verification process. Users who feel more at ease and safe with CBIOSCT will be more likely to show an increased interest in adopting this type of technology in current forms of identification for identity theft and fraud prevention.

Recommendations for Future Research

This investigation required that the research site included residents of the most visited cities by tourists throughout the United States, due to the ease with which incidents of security such as theft, domestic, international, and cross-border terrorism could occur (Mansfeld & Pizam, 2006). The investigation was delimited to the sample that was representative of the intended population: people residing in New York, NY; Washington, DC; Orlando, FL, Charleston, SC; Las Vegas, NV; and San Francisco, CA. These cities were selected from the importance ranking of U.S. cities most visited by tourists (TripAdvisor, 2016). Therefore, the sample of this investigation is not a true generalizable representation of the U.S. public's behavioral intention to use CBIOSCT. However, the research findings offer important insight into understanding the U.S. public's perspectives of CBIOSCT at multiple tourist destinations throughout the U.S. It is recommended that future research expand beyond tourist destination cities in the U.S. to other cities where people are vulnerable to identity crimes. This should provide a better understanding of the U.S. public's attitudes and their perceptions to adopting CBIOSCT in existing forms of personal identification.

The research findings showed that SI is not a determining factor of the U.S. public's intentions to adopt a CBIOSCT in current forms of ID at multiple tourist destinations throughout the U.S. This outcome suggests that people's willingness to adopt this technology depend, in part, upon whether they perceive that they are adequately provided with the appropriate infrastructure and knowledge. Therefore, it would be valuable to expand the UTAUT model to test the influence of other determinants of technology adoption, such as awareness, trust (Miltgen et al., 2013), privacy concerns, and information sensitivity (Morosan, 2016). Future research should also examine the extent to which people's attitudes toward the adoption of CBIOSCT is

mediated by the FC factor, as this study found a significant correlation between FC and Att that was not postulated in this study. Other directions of research may include investigating the moderating effect of design, security solutions, service and maintenance on facilitating conditions and whether the role of these factors outweighs the negative effect of privacy and risk perceptions. Finally, qualitative research could also be conducted to further improve the model and to better understand what influences people's positive and negative perceptions of CBIOSCT in current forms of identification to prevent identity theft and fraud.

Conclusion

This nonexperimental correlational quantitative investigation aimed to examine the factors that influence the U.S. public's acceptance of CBIOSCT in current forms of identification for identity theft and identity fraud prevention. To better comprehend acceptance of this technology, the UTAUT model was used and expanded to test five explanatory factors: PE, PC, SI, FC, and Att. Findings of the SEM parsimonious model indicated that Att was the strongest predictor of the U.S. public's intention to use CBIOSCT. Results of the SEM analysis also disclosed a positive effect of FC on the U.S. public's intention to use CBIOSCT. Finally, the study results showed a significant correlation between FC and Att, which was not hypothesized in this study, indicating that the public's attitudes towards the use of CBIOSCT pivot around the existence of adequate infrastructure. Likewise, this research revealed that PC was an intermediary factor in explaining the changes of the PE factor.

To address the identified determinant factors for adopting CBIOSCT in current forms of identification, this study recommended that the government and any institution that requires identity verification of individuals should (1) spend more on biometric and smart card infrastructure set up, hotline, maintenance, and updates, (2) raise awareness regarding the

objectives, features, impact, available resources, and advantages of CBIOSCT through the dissemination of this information to the public, and (3) devise and enforce tailor-made policies and measures for validating and confirming the cardholder's identity, safeguarding the cardholder's information, and alerting inconsistencies in the cardholder's authentication process. Furthermore, future research could expand the UTAUT model to test the influence of other determinants of technology adoption and examine the extent to which people's attitude towards the adoption of the technology is mediated by the FC factor, as this study found a significant correlation between FC and Att.

This study's findings have important theoretical and practical implications. From a theoretical standpoint, empirical evidence of this study revealed that the UTAUT model is suitable for studying the determinants of CBIOSCT adoption and use, since the extended UTAUT model used in this research accounted for 73% of the variance in BI to use CBIOSCT. From a practical viewpoint, the results of this study offer scholars and practitioners important insights into understanding the U.S. public's perspectives of CBIOSCT at multiple tourist destinations throughout the United States. Understanding the factors influencing user acceptance of CBIOSCT in current forms of identification for identity theft and fraud prevention would enable lawmakers, organizations, financial institutions, and identity management service providers to devise suitable future provisions and policy measures to tackle the challenges identity theft crimes pose. Equipping the public with pertinent information and resources will lead to more positive attitudes toward the technology, which may translate into adoption of CBIOSCT in current forms of ID in the United States.

References

- Abdollahzadeh, G., Ahmadi-Gorgi, H., Damalas, C. A., & Sharifzadeh, M. S. (2017). Predicting adoption of biological control among Iranian rice farmers: An application of the extended technology acceptance model (TAM2). *Crop Protection*, 96, 88-96. doi:10.1016/j.cropro.2017.01.014
- Abduljalil, K., & Zainuddin, Y. (2015). Intrinsic and extrinsic motivation as attitude factors towards adoption of accounting information system (AIS) in Libyan SMEs. *International Journal of Academic Research in Accounting, Finance, and Management Sciences*, 5(1), 161-170. doi:10.6007/IJARAFMS/v5-i1/1553
- Acquisti, A., Romanosky, S., & Telang, R. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis & Management*, 30(2), 256-286. doi:10.1002/pam.20567
- Addo, H., & Attuquayefio, S. (2014a). Review of studies with UTAUT as conceptual framework. *European Scientific Journal*, 10(8), 249-258. Retrieved from <https://ejournal.org/index.php/esj>
- Addo, H., & Attuquayefio, S. N. (2014b). Using the UTAUT model to analyze students' ICT adoption. *International Journal of Education and Development using Information and Communication Technology*, 10(3), 75-86. Retrieved from <http://ijedict.dec.uwi.edu/>
- Agbaraji, C. E., Agwah, C. B., & Ezetoha, F. (2014). National identification issues and the solution using smart card technology. *International Journal of Engineering Research & Technology (IJERT)*, 3(8), 314-320. Retrieved from <http://www.ijert.org/>
- Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods*, 17(4), 351-371. doi:10.1177/1094428114547952
- Ahmed, H., Basoglu, N., & Daim, T. (2007). Information technology diffusion in higher education. *Technology in Society*, 29(4), 469-482. doi:10.1016/j.techsoc.2007.08.011
- Ahn, T., Han, I., & Ryu, S. (2007). The impact of web quality and playfulness on user acceptance of online retailing. *Information & Management*, 44, 263-275. doi:10.1016/j.im.2006.12.008
- Ahn, S., Jin, Y., Myers, N. D. (2011). Sample size and power estimates for a confirmatory factor analytic model in exercise and sport: A Monte Carlo approach. *Research Quarterly for Exercise and Sport*, 82(3), 412-423. doi:10.1080/02701367.2011.10599773
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50(2), 179-211. Retrieved from <https://www.journals.elsevier.com>

- Ajzen, I., & Fishbein, M. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Akman, I., Mishra, A., & Mishra, D. (2014). Theory of reasoned action application for green information technology acceptance. *Computers in Human Behavior*, 36, 29-40. doi:10.1016/j.chb.2014.03.030
- Al-Abdallah, G. M., & Al-Qeisi, K. I. (2014). Website design and usage behaviour: An application of the UTAUT model for Internet banking in UK. *International Journal of Marketing Studies*, 6(1), 75-89. doi:10.5539/ijms.v6n1p75
- Al-Khouri, A. M. (2013). Critical insights from a practitioner mindset. *Thoughts with impact series*. (Vol. 3). Oxford, England: Chartridge Books Oxford.
- AlGhamdi, R., Alhussain, T., Alshehri, M., & Drew, S. (2012). Analysis of citizen's acceptance for e-government services: Applying the UTAUT model. *Proceedings of the IADIS International Conferences Theory and Practice in Modern Computing and Internet Applications and Research, Lisbon, Portugal*, 69-76.
- Ali, M., El-Masri, M., Serrano, A., & Tarhini, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of Internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, 29(4), 830-849. doi:10.1108/ITP-02-2014-0034
- Ali, S. W., & Wani, T. A. (2015). Innovation diffusion theory: Review & scope in the study of adoption of smartphones in India. *Journal of General Management Research*, 3(2), 101-118. Retrieved from <https://www.scmsnoida.ac.in/>
- Alkhurayyif, Y. (2013). National ID cards. *International Journal of Computing Science and Information*, 1(2), 44-48. Retrieved from <http://airccse.org/journal/ijcsit.html>
- Allen, C., Gaffar, K., Gajraj, R., Jackman, G. A., Singh, L., Thakur, D., ... & Tooma, K. (2014). Measurement invariance of the UTAUT constructs in the Caribbean. *International Journal of Education and Development Using Information and Communication Technology (IJEDICT)*, 10(4), 102-127. Retrieved from <http://ijedict.dec.uwi.edu/>
- Alonso-Bejarano, C., & Goldstein, D. M. (2017). E-Terrify: Securitized immigration and biometric surveillance in the workplace. *Human Organization*, 76(1), 1-14. doi:10.17730/0018-7259.76.1.1
- American Psychological Association. (2010). *Ethical principles of psychologists and code of conduct: Including 2010 and 2016 amendments*. Retrieved from <http://www.apa.org/ethics/code/>

- Anderson, R. E., Babin, B. J., Black, W. C., Hair, J. F., Jr. (2014). *Multivariate data analysis* (7th ed.). Edinburgh Gate, England: Pearson Education Limited.
- Andrus, M. T. (2017). Not without my consent: Preserving individual liberty in light of the comprehensive collection and consolidation of personally identifiable information. *Journal of Internet Law*, 20(9), 1-27. Retrieved from <https://lrus.wolterskluwer.com/>
- Archer, & Gilbert. (2012). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime*, 19(1), 20-36. doi:10.1108/13590791211190704
- Ariff, M. S. M., Ishak, N., Ismail, K., Min, Y. S., & Zakuan, N. (2013). The impact of computer self-efficacy and technology acceptance model on behavioral intention in Internet banking system. *Review of Integrative Business & Economics Research*, 2(2), 587-601. Retrieved from <http://sibresearch.org/riber.html>
- Asparouhov, T., Morin, A. J. S., & Muthén, B. (2015). Bayesian structural equation modeling with cross-loadings and residual covariances: Comments on Stromeier et al. *Journal of Management*, 41(6), 1561-1577. doi:10.1177/0149206315591075
- Babalhavaeji, F., Khosravi, F., & Nazari, F. (2013). Applying Rogers' diffusion of innovation theory to the acceptance of online databases at University Zone of Iran. *Malaysian Journal of Library & Information Science*, 18(3), 25-38. Retrieved from <https://jice.um.edu.my/index.php/MJLIS/index>
- Bae, S., He, Q., Lillard, J. W., Jr., Mayberry, R., Singh, K., & Yoo, W. (2014). A study of effects of multicollinearity in the multivariable analysis. *International Journal of Applied Science and Technology*, 4(5), 9-19. Retrieved from <http://www.ijastnet.com/>
- Baechler, S., Fritz, T., Ribaux, O., Pierre, M., Pujol, J., & Terrasse, V. (2013). The systematic profiling of false identity documents: Method validation and performance evaluation using seizures known to originate from common and different sources. *Forensic Science International*, 232, 180-190. doi:10.1016/j.forsciint.2013.07.022
- Bagozzi, R. P., Davis, F. D., Warshaw, P.R. (1989). User acceptance of computer acceptance: A comparison of two theoretical models. *Management Science*, 35, 982-1003. doi:10.1287/mnsc.35.8.982
- Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology*, 22(14), 1111-1132. doi:10.1111/j.1559-1816.1992.tb00945.x
- Bali, V. (2009). Tinkering toward a national identification system: An experiment on policy attitudes. *Policy Studies Journal*, 37(2), 233-255. doi:10.1111/j.1541-0072.2009.00312.x

- Balasubramanian, S. A., Kasilingam, D. L., & Natarajan, T. (2017). Understanding the intention to use mobile shopping applications and its influence on price sensitivity. *Journal of Retailing and Consumer Services*, 37, 8-22. doi:10.1016/j.jretconser.2017.02.010
- Bănărescua, A. (2015). Detecting and preventing fraud with data analytics. *Procedia Economics and Finance*, 32, 1827-1836. doi:10.1016/S2212-5671(15)01485-9
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.
- Baptista, G., Campos, F., Oliveira, T., & Thomas, M. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, 61, 404-414. doi:10.1016/j.chb.2016.03.030
- Bargh, J. A., Gollwitzer, P. M., & Sheeran, P. (2013). Nonconscious processes and health. *Health Psychology*, 32(5), 460-473. doi:10.1037/a0029203
- Baroudi, J. J., Igbaria, M., & Parasuraman, S. (1996). A Motivational Model of Microcomputer Usage. *Journal of Management Information Systems*, 13(1), 127-143. doi:10.1080/07421222.1996.11518115
- Bastos, J. L., Bonamigo, R. R., Duquia, R. P., González-Chica, D. A., & Mesa, J. M. (2014). Field work I: Selecting the instrument for data collection. *Anais Brasileiros de Dermatologia*, 89(6), 918-923. doi:10.1590/abd1806-4841.20143884
- Batane, T., & Motshegwe, M. M. (2015). Factors influencing instructors' attitudes toward technology integration. *Journal of Educational Technology Development & Exchange*, 8(1), 1-16. Retrieved from <http://jetde.theti.org>
- Bayaga, A., & Nyembezi, N. (2014). Performance expectancy and usage of information systems and technology: Cloud computing (PEUISTCC). *International Journal of Educational Sciences*, 7(3), 579-586. Retrieved from http://www.krepublishers.com/journals_educationalscience.html
- Belanche, D., Casaló, L. V., & Flavián, C. (2014). The role of place identity in smart card adoption. *Public Management Review*, 16(8), 1205-1228. doi:10.1080/14719037.2013.792385
- Belanche-Gracia, D., Casaló-Ariño, L. V., & Pérez-Rueda, A. (2015). Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Government Information Quarterly*, 32, 154-163. doi:10.1016/j.giq.2014.12.004

- Bell, A., & Ramsey, K. (2014). The smart location database: A nationwide data resource characterizing the built environment and destination accessibility at the neighborhood scale. *Cityscape: A Journal of Policy Development & Research*, 16(2), 145-162. Retrieved from <https://www.huduser.gov/portal/periodicals/cityscape.html>
- Benbasat, I., & Moore, G. C. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, 2(3), 192-222. doi:1047-7047/91/0203/0192/
- Benjamin, A. C., Emmanuel, A. C., & Franklin, E. (2014). National identification issues and the solution using smart card technology. *International Journal of Engineering Research & Technology (IJERT)*, 3(8), 314-320. Retrieved from <http://www.ijert.org/>
- Bengtsson, L., & Sällberg, H. (2016). Computer and smartphone continuance intention: A motivational model. *Journal of Computer Information Systems*, 56(4), 321-330. doi:10.1080/08874417.2016.1164007
- Berg, C. J., Bierut, L. J., Cavazos-Rehg, P. A., Krauss, M. J., Sehi, A., Sowles, S. J., & Spitznagel, E. L. (2017). Marijuana advertising exposure among current marijuana users in the U.S. *Drug and Alcohol Dependence*, 174, 192-200. doi:10.1016/j.drugalcdep.2017.01.017
- Bertino, E., Huang, X., Xiang, Y., Xu, L., & Zhou, J. (2014). Robust multi-factor authentication for fragile communications. *IEEE Transactions on Dependable and Secure Computing, Dependable and Secure Computing*, 11(6), 568-581. doi:10.1109/TDSC.2013.2297110
- Bilgihan, A., Khalilzadeh, J., & Ozturk, A. B. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, 70, 460-474. doi:10.1016/j.chb.2017.01.001
- Bonnar-Kidd, K. K. (2010). Sexual offender laws and prevention of sexual violence or recidivism. *American Journal of Public Health*, 100(3), 412-419. doi:10.2105/AJPH.2008.153254
- Borza, D., Danescu, R., & Darabant, A. S. (2013). Eyeglasses lens contour extraction from facial images using an efficient shape description. *Sensors*, 13(10), 13638-13658. doi:10.3390/s131013638
- Bozbeyoğlu, A. C. (2011). Citizenship rights in a surveillance society: The case of the electronic ID card in Turkey. *Surveillance & Society*, 9, 64-79. Retrieved from <http://surveillance-and-society.org/>
- Bradbury, D. (2016). Fighting ID theft. *Engineering & Technology*, 10(12), 60-63. Retrieved from <https://eandt.theiet.org/>

- Breckler, S. J. (1990). Applications of covariance structure modeling in Psychology: Cause for concern? *Psychological Bulletin*, 107(2), 260-273. doi:10.1037/0033-2909.107.2.260
- Brenčič, M. M., Cimperman, M., & Trkman, P. (2016). Analyzing older users' home telehealth services acceptance behavior—Applying an extended UTAUT model. *International Journal of Medical Informatics*, 90, 22-31. doi:10.1016/j.ijmedinf.2016.03.002
- Briller, V., Han, H. J., & Hiltz, S. R. (2003). Public attitudes towards a national identity smartcard: Privacy and security concerns. In *Proceedings of the 36th Hawaii International Conference on System Sciences, USA* (pp. 1-8). doi:10.1109/HICSS.2003.1174312
- Brooks, M. (2013). For nontraditional names' sake: A call to reform the name-change process for marrying couples. *University of Michigan Journal of Law Reform*, 47(1), 247-282. Retrieved from <https://mjl.org/>
- Brown, T. A. (2015). *Confirmatory factor analysis for applied research* (2nd. ed.). In T. D. Little (Ed.). New York, NY: Guilford Press.
- Brown, S. A., Chan, F. Y., Hu, P. J., Tam, K. Y., Thong, J. Y. L., & Venkatesh, V. (2010). Modeling citizen satisfaction with mandatory adoption of an e-government technology. *Journal of the Association for Information Systems*, 11(10), 519-549. Retrieved from <http://aisel.aisnet.org/jais/>
- Brown, R., Emami, C., & Smith, R. G. (2016). Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia. *Trends & Issues in Crime & Criminal Justice*, 511, 1-6. Retrieved from <http://aic.gov.au/>
- Brownlow, C., Hinton, P. R., & McMurray, I. (2014). *SPSS explained* (2nd ed.). New York, NY: Routledge.
- Bush, R., Cole, M. L., & Kohnke, A. (2014). Incorporating UTAUT predictors for understanding home care patients' and clinician's acceptance of healthcare telemedicine equipment. *Journal of Technology Management & Innovation*, 9(2), 29-41. doi:10.4067/S0718-27242014000200003
- Button, K. S., Flint, J., Ioannidis, J. P., Mokrysz, C., Munafò, M. R., Nosek, B. A., & Robinson, E. S. (2013). Power failure: Why small sample size undermines the reliability of neuroscience. *Nature Reviews Neuroscience*, 14(5), 365-376. doi:10.1038/nrn3475
- Bytha, A., Khechine, H., Lakhal, S., & Pascot, D. (2014). UTAUT model for blended learning: the role of gender and age in the intention to use webinars. *Interdisciplinary Journal of E-Learning & Learning Objects*, 10, 33-52. Retrieved from <http://www.ijello.org/>

- Byun, S., & Byun, S. E. (2013). Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behavior & Information Technology*, 32(3), 217-230. doi:10.1080/0144929X.2011.553741
- Calhoun, M. P. (2016). DARPA emerging technologies. *Strategic Studies Quarterly*, 10(3), 91-113. Retrieved from <http://www.airuniversity.af.mil/SSQ/>
- Cano, S. M., Sass, D. A., & Tumlinson, S. E. (2014). The search for causal inferences: Using propensity scores post hoc to reduce estimation error with nonexperimental research. *Journal of Pediatric Psychology*, 39(2), 246-257. doi:10.1093/jpepsy/jst143
- Carpenter, D., Chen, X., Hicks, C., & Maasberg, M., (2016). A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system. *International Journal of Information Management*, 36, 735-747. doi:10.1016/j.ijinfomgt.2016.02.013
- Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2014). Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model. *Tourism Management*, 43, 70-88. doi:10.1016/j.tourman.2014.01.017
- Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal*, 18(2), 69-110. doi:10.4314/pelj.v18i2.02
- Castro, D. (2011). Explaining international leadership: Electronic identification systems. *The Information Technology & Innovation Foundation*. Retrieved from <http://www.itif.org/files/2011-e-id-report-final.pdf>
- Chau, P. K., Hu, P. J., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the technology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems*, 16(2), 91. Retrieved from <http://www.jmis-web.org/issues>
- Chauhan, S., & Jaiswal, M. (2016). Determinants of acceptance of ERP software training in business schools: Empirical investigation using UTAUT model. *International Journal of Management Education*, 14(3), 248-262. doi:10.1016/j.ijme.2016.05.005
- Chen, Z., Cheung, C. M. K., & Lee, M. K. O. (2005). Acceptance of Internet-based learning medium: The role of extrinsic and intrinsic motivation. *Information and Management*, 42(8), 1095-1104. doi:10.1016/j.im.2003.10.007
- Chieh-Heng, K., & Chun-Chieh, Y. (2015). Exploring employees' perception of biometric technology adoption in hotels. *International Journal of Organizational Innovation*, 8(2), 187-199. Retrieved from <http://www.ijoi-online.org/>

- Ching-Wei, H., Yen, N. Y., & Yu-Bing, W. (2015). Does environmental sustainability play a role in the adoption of smart card technology at universities in Taiwan: An integration of TAM and TRA. *Sustainability*, 7(8), 10994-11009. doi:10.3390/su70810994
- Choi, J. G., Ham, S., Kim, E., & Yang, I. S. (2013). The roles of attitude, subjective norm, and perceived behavioral control in the formation of consumers' behavioral intentions to read menu labels in the restaurant industry. *International Journal of Hospitality Management*, 35, 203-213. doi:10.1016/j.ijhm.2013.06.008
- Chong, S. C., Loo, W. H., & Yeow, P. H. P. (2009). User acceptance of Malaysian government multipurpose smartcard applications. *Government Information Quarterly*, 26(2), 358-367. doi:10.1016/j.giq.2008.07.004
- Chong, S. C., Loo, W. H., & Yeow, P. P. (2011). Acceptability of multipurpose smart national identity card: An empirical study. *Journal of Global Information Technology Management*, 14(1), 35-58. doi:10.1080/1097198X.2011.10856530
- Claydon, L. S. (2015). Rigour in quantitative research. *Nursing Standard*, 29(47), 43-48. doi:10.7748/ns.29.47.43.e8820
- Cleveland, M., Hille, P., & Walsh, G. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, 30, 1-19. doi:10.1016/j.intmar.2014.10.001
- Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17(3), 181-188. doi:10.1016/j.jretconser.2010.03.007
- Clough, J. (2015). Towards a common identity? The harmonization of identity theft laws. *Journal of Financial Crime*, 22(4), 492-512. doi:10.1108/JFC-11-2014-0056
- Cohen, J. (1992). Statistical power Analysis. *Current Direction in Psychological Science*, 1(3), 98-101. Retrieved from <http://www.psychologicalscience.org/>
- Committee on Communication for Behavior Change in the 21st Century (2002). *Speaking of health: Assessing health communication strategies for diverse populations*. Washington, DC: National Academies Press.
- Copes, H., Pike, A., Powell, Z. A., & Vieraitis, L. M. (2015). A little information goes a long way: Expertise and identity theft. *Aggression and Violent Behavior*, 20, 10-18. doi:10.1016/j.avb.2014.12.008
- Costello, A. B. and Osborne, J. W. (2005) Best practices in exploratory factor analysis: four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation*, 10(7), 1-9. Retrieved from <https://pareonline.net/>

- Cottrell, R. R., & McKenzie, J. F. (2011). *Health promotion & education research methods: Using the five chapter thesis/dissertation model*. Sudbury, MA: Jones & Bartlett Learning.
- Council of the European Union. (2010). *State of play concerning the electronic identity cards in the EU member states* (9949/10 FAUXDOC 10 COMIX 373). Retrieved from <http://www.statewatch.org/news/2010/jun/eu-council-ID-cards-9949-10.pdf>
- Cybersecurity Information Sharing Act of 2015, 754 S. §103. (2015).
- Das, A. K., Goswami, A., & Odelu, V. (2015). An efficient biometric-based privacy-preserving three-party authentication with key agreement protocol using smart cards. *Security and Communication Networks*, 8, 4136-4156. doi:10.1002/sec.1330
- Das, A. K., Mishra, D., & Mukhopadhyay, S. (2014). A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Systems with Applications*, 41, 8129-8143. doi:10.1016/j.eswa.2014.07.004
- Das, R. (2016). *Adopting biometric technology: Challenges and solutions*. Boca Raton, FL: Taylor & Francis Group.
- Dash, R., & Mishra, M. K. (2014). A comparative study of Chebyshev functional link artificial neural network, multi-layer perceptron and decision tree for credit card fraud detection. *Proceedings of the International Conference on Information Technology (ICIT), IEE Computer Society*, 228-233. doi:10.1109/ICIT.2014.25
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-339. Retrieved from <http://www.misq.org/>
- Davis, F. D., Davis, G. B., Morris, M. G., & Venkatesh, V. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, 27(3), 425-478. Retrieved from <http://www.misq.org/>
- Davis, F. D., & Venkatesh, V. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204. Retrieved from <https://pubsonline.informs.org/journal/mnsc>
- De Kerviler, G., Demoulin, N. T., & Zidda, P. (2016). Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? *Journal of Retailing and Consumer Services*, 31, 334-344. doi:10.1016/j.jretconser.2016.04.011
- Dečman, M. (2015). Modeling the acceptance of e-learning in mandatory environments of higher education: The influence of previous education and gender. *Computers in Human Behavior*, 49, 272-281. doi:10.1016/j.chb.2015.03.022

- Deci, E.L., & Ryan, R.M. (1985). *Intrinsic motivation and self-determination in human behavior* [Adobe Digital Editions version]. doi:10.1007/978-1-4899-2271-7
- Devadas, S., & Meng-Day (Mandel), Y. (2017). Pervasive, dynamic authentication of physical items. *Communications of the ACM*, 60(4), 32-39. doi:10.1145/3024922
- Doane, A. N., Kelley, M. L., & Pearson, M. R. (2014). Predictors of cyberbullying perpetration among college students: An application of the theory of reasoned action. *Computers in Human Behavior*, 36, 154-162. doi:10.1016/j.chb.2014.03.051
- Dolnicar, S. (2013). Asking good survey questions. *Journal of Travel Research*, 52(5), 551-574. doi:10.1177/0047287513479842
- Don, Y., & Raman, A. (2013). Preservice teachers' acceptance of learning management software: An application of the UTAUT2 model. *International Education Studies*, 6(7), 157-164. doi:10.5539/ies.v6n7p157
- Donovan, K. P., & Martin, A. K. (2015). New surveillance technologies and their publics: A case of biometrics. *Public Understanding of Science*, 24(7), 842-857. doi:10.1177/0963662513514173
- Doody, O., & Noonan, M. (2016). Nursing research ethics, guidance and application in practice. *British Journal of Nursing*, 25(14), 803-807. doi: 10.12968/bjon.2016.25.14.803
- Dowd, J., Joa, C. Y., Magsamen-Conrad, K., & Upadhyaya, S., (2015). Bridging the divide: Using UTAUT to predict multigenerational tablet adoption practices. *Computers in Human Behavior*, 50, 186-196. doi:10.1016/j.chb.2015.03.032
- Draper, R., Prenzler, T., & Ritchie, J. (2012). Making the most of security technology. In T. Prenzler (Ed.), *Policing and security in practice: Challenges and achievements* (pp. 186-203). New York, NY: St Martin's Press.
- Driver's Privacy Protection Act, 18 U.S.C. §§ 2720-2721 (1993).
- Du, C., Lin, H., & Wen, F. (2015). An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics. *Wireless Personal Communications*, 84, 2351-2362. doi:10.1007/s11277-015-2708-4
- Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2014). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management*, 28(3), 443-488. doi:10.1108/JEIM-09-2014-0088
- Ehteshami, A. (2017). Barcode technology acceptance and utilization in health information management department at academic hospitals according to technology acceptance model. *Acta Informatica Medica*, 25(1), 4-8. doi:10.5455/aim.2017.25.4-8

- Elbeck, M. M. (2014). Selecting a free web-hosted survey tool for student use. *E-Journal of Business Education & Scholarship of Teaching*, 8(2), 54-68. Retrieved from <http://www.ejbest.org>
- Electronic Privacy Information Center. (2017, January). *EPIC urges TSA to drop REAL ID data collection plan*. Retrieved from https://epic.org/privacy/id_cards/
- Electronic Privacy Information Center. (n.d.). *Social security numbers*. Retrieved from <https://www.epic.org/privacy/ssn/>
- Eramo, L. A. (2011). Stopping fraud: Detecting and preventing fraud in the e-Health era. *Journal of AHIMA*, 82(3), 28-30. Retrieved from <http://journal.ahima.org/>
- Fagnäs, S. (2014). Papers, please! The effect of birth registration on child labor and education in early 20th century USA. *Explorations in Economic History*, 52, 63-92. doi:10.1016/j.eeh.2013.09.002
- Fahl, S., Harbach, M., Smith, M., Rieger, M. (2013). On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. *Privacy Enhancing Technologies*, 7981, 1-20, doi:10.1007/978-3-642-39077-7_13
- Fain, J. A. (2017) *Reading, understanding, and applying nursing research* (5th ed.). Philadelphia, PA: F. A. Davis
- Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 112, 114, 154 (2003).
- Fair Credit Reporting Act, 15 USC § 1681 (1970).
- Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692-1692p (2010).
- Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974).
- Fascendini, F., & Roveri, F. (2014). "Your software is my biology": The mass surveillance system in Argentina. *Global Information Society Watch*, 61-64. Retrieved from <http://www.giswatch.org/en/country-report/communications-surveillance/argentina>
- Federal Public Service for Information and Communication Technology. (2012). *The electronic identity documents*. Retrieved from <http://eid.belgium.be/en/>
- Federal Trade Commission. (2012). *How to keep your personal information secure*. Retrieved from <https://www.consumer.ftc.gov/>

- Federal Trade Commission. (2017). *Consumer sentinel network: Data book for January – December 2016*. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf
- Federal Trade Commission Identity Theft Rules, 16 C.F.R. § 681, 72 FR 63771-63772 (2007).
- Fell, J., Romano, E., Scherer, M., & Taylor, E. (2015). A comprehensive examination of U.S. laws enacted to reduce alcohol-related crashes among underage drivers. *Journal of Safety Research*, 55, 213-221. doi:10.1016/j.jsr.2015.08.001
- Fidell L. S., and Tabachnick, B. G. (2014). *Using multivariate statistics* (6th ed.). Edinburgh Gate, England: Pearson Education Limited.
- Field, A., & Miles, J. (2010). *Discovering statistics using SAS*. Thousand Oaks, CA: SAGE Publications Inc.
- Fliegelman, O. (2015, February 6). Made in China: Fake IDs. *The New York Times*. Retrieved from <https://www.nytimes.com>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50. doi:10.2307/3151312
- Franks, H., Krause, J. M., & Lynch, B. (2017). Current technology trends and issues among health and physical education professionals. *Physical Educator*, 74(1), 164-180. doi:10.18666/TPE-2017-V74-I1-6648
- Friedewald, M., & Pohoryles, R. J. (2013). Technology and privacy. *Innovation: The European Journal of Social Sciences*, 26(1/2), 1-6. doi:10.1080/13511610.2013.768011
- Friedline, T. (2016). Building bridges, removing barriers: The unacceptable state of households' financial health and how financial inclusion can help. *University of Kansas, Center on Assets, Education, and Inclusion* (pp. 1-83). Retrieved from <https://aedi.ku.edu/>
- Gaffar, K., Singh, L., & Thomas, T. D. (2013). The utility of the UTAUT model in explaining mobile learning adoption in higher education in Guyana. *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 9(3), 71-85. Retrieved from <http://ijedict.dec.uwi.edu/>
- Garfinkel, S. L. (2015). De-identification of personal information (NISTIR Publication No. 8053). *U.S. Department of Commerce, National Institute of Standards and Technology*, 1-46. doi:10.6028/NIST.IR.8053

- Garza, G., & Landrum, B. (2015). Mending fences: Defining the domains and approaches of quantitative and qualitative research. *Qualitative Psychology*, 2, 199-209. doi:10.1037/qup0000030
- Gaurav, J., Ranjan, J., & Tyagi, S. (2012). An intuitive approach to prevent smart card fraud using fingerprinting authentication and enhanced data encryption standard (EHDES). *International Journal of Computer Applications* (0975 – 8887), 40(16), 6-10. doi:10.5120/5062-7222
- Giumetti, G. W., Kowalski, R. M., Lattanner, M. R., & Schroeder, A. N. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073-1137. doi:10.1037/a0035618
- Gramm-Leach-Bliley Act, 12 U.S.C. § 1811 (1999).
- Granić, A., & Marangunić, N. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, 14(1), 81-95. doi:10.1007/s10209-014-0348-1
- Gravetter, F., & Wallnau, L. (2014). *Essentials of statistics for the behavioral sciences* (8th ed.). Belmont, CA: Wadsworth.
- Guadagnoli, E., & Velicer, W. F. (1988). Relation of sample size to the stability of component patterns. *Psychological Bulletin*, 103(2), 265-275. doi:10.1037/0033-2909.103.2.265
- Gunawardena, C. G., & Samaradiwakara, G. D. M. N. (2014). Comparison of existing technology acceptance theories and models to suggest a well improved theory/model. *International Technical Sciences Journal (ITSJ)*, 1(1), 21-36. Retrieved from <http://bsrun.org/news/call-papers-international-technical-sciences-journal-itsj-2015>
- Gunaydin, S., & McCusker, K. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, 30(7), 537-542. doi:10.1177/0267659114559116
- Hao-Hsien, L., Hui-Man, H., & Lee-Jen, W. S. (2014). A comparison of convenience sampling and purposive sampling. *Journal of Nursing*, 61(3), 105-111. doi:10.6224/JN.61.3.105
- Harby, F. A., Kamala, M., & Qahwaji, R. (2012). End-users' acceptance of biometrics authentication to secure e-commerce within the context of Saudi culture: Applying the UTAUT model. In R. Pande & T. Van der Weide (Eds.), *Globalization, technology diffusion and gender disparity: Social impacts of ICTs* (pp. 225-246). doi:10.4018/978-1-4666-0020-1

- Harinda, E., & Ntagwirumugara, E. (2015). Security & privacy implications in the placement of biometric-based id card for Rwanda universities. *Journal of Information Security*, 6, 93-100. doi:10.4236/jis.2015.62010
- Harsono, I. L. D., & Suryana, L. A. (2014). Factors affecting the use behavior of social media using UTAUT 2 model. *Proceedings of the First Asia-Pacific Conference on Global Business, Economics, Finance and Social Sciences, Singapore, S471*, 1-14. Retrieved from <http://globalbizresearch.org/>
- Health Insurance Portability and Accountability Act, 45 C.F.R. §§164.502-164.514 (1996).
- Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution*, 4(1), 1-12. doi:10.5897/JLCR11.044
- Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society*, 44, 30-38. doi:10.1016/j.techsoc.2015.11.007
- Hermida, R. (2015). The problem of allowing correlated errors in structural equation modeling: Concerns and considerations. *Computational Methods in Social Sciences*, 3(1), 1-17. Retrieved from <http://cmss.univnt.ro/>
- Higgins, C. A., Howell, J. M., & Thompson, R. L. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly*, 15(1), 125-143. Retrieved from <http://www.misq.org/>
- Hino, H. (2015). Assessing factors affecting consumers' intention to adopt biometric authentication technology in e-shopping. *Journal of Internet Commerce*, 14, 1-20. doi:10.1080/15332861.2015.1006517
- Ho, A. T., & Ni, A. Y. (2008). A quiet revolution or a flashy blip? The Real ID Act and U.S. national identification system reform. *Public Administration Review*, 68(6), 1063-1078. doi:10.1111/j.1540-6210.2008.00955.x
- Hoewe, J., & Sherrick, B. (2015). Using the theory of reasoned action and structural equation modeling to study the influence of news media in an experimental context. *Atlantic Journal of Communication*, 23(5), 237-253. doi:10.1080/15456870.2015.1090276
- Hong, S., MacCallum, R. C., Widaman, K. F., & Zhang, S. (1999). Sample size in factor analysis. *Psychological Methods*, 4(1), 84-99. doi:10.1037/1082-989x.4.1.84
- Horrey, W. J., Lesch, M. F., Rahman, M. M., & Strawderman, L. (2017). Assessing the utility of TAM, TPB, and UTAUT for advanced driver assistance systems. *Accident Analysis and Prevention*, 108, 361-373. doi:10.1016/j.aap.2017.09.011

- Hosein, G., Martin, A. K., & Whitley E. A. (2014). From surveillance-by-design to privacy-by-design: Evolving identity policy in the UK. In K. Boersma, R. van Brakel, C. Fonio C, & P. Wagenaar (Eds.), *Histories of state surveillance in Europe and beyond* (pp. 205-219). New York, NY: Routledge.
- Hou, C. (2014). Exploring the user acceptance of business intelligence systems in Taiwan's electronics industry: Applying the UTAUT model. *International Journal of Internet & Enterprise Management*, 8(3), 195–226. doi:10.1504/IJIEEM.2014.059177
- Howard, A. L. (2013). Handbook of structural equation modeling. *Structural Equation Modeling: A Multidisciplinary Journal*, 20(2), 354-360. doi:10.1080/10705511.2013.769397
- Hsieh, C. T., Lai, F., & Li, D. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52, 353-363. doi:10.1016/j.dss.2011.09.002
- Hu, M. (2013). Biometric ID cybersurveillance. *Indiana Law Journal*, 88(4), 1475-1558. Retrieved from <http://ilj.law.indiana.edu/>
- Hughley K., & Jator, E. K. (2014). ABO/Rh testing, antibody screening, and biometric technology as tools to combat insurance fraud: An example and discussion. *Laboratory Medicine*, 45(1), e3-e7. doi:10.1309/LMIEC52ZF7RLLURK
- Hwang, H., Kim, S., Lee, K., & Yoo, S. (2016). Analysis of the factors influencing healthcare professionals' adoption of mobile electronic medical record (EMR) using the unified theory of acceptance and use of technology (UTAUT) in a tertiary hospital. *BMC Medical Informatics and Decision Making*, 16(1), 12. doi:10.1186/s12911-016-0249-8
- Hwang, Y., Lee, S., & Shin, D. (2017). How do credibility and utility play in the user experience of health informatics services? *Computers in Human Behavior*, 67, 292-302. doi:10.1016/j.chb.2016.11.007
- Identity systems and civil registration in Asia. (2017). *Population and Development Review*, 43(1), 183-187. doi:10.1111/padr.12040
- Identity Theft and Assumption Deterrence Act, 4151. H.R. 18 U.S.C. §1028 (1998).
- Identity Theft Enforcement and Restitution Act, Pub. L. No. 110-326, title II, §§ 202-203, 122 Stat. 3561 (2008).
- Identity Theft: How to protect and restore your good name: Hearings before the Subcommittee on Technology, Terrorism, and Government Information*, Senate, 106 Cong. (2000) (Testimony of Beth Givens).

- Identity Theft Penalty Enhancement Act of 2004, Pub. L. No. 108–275 § 1028A, 150 Stat. 831 (2004).
- Identity Theft Resource Center. (2017, January). *Data breach reports: 2016 end of year report*. Retrieved from http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf
- Ifinedo, P. (2017). Examining students' intention to continue using blogs for learning: Perspectives from technology acceptance, motivational, and social-cognitive frameworks. *Computers in Human Behavior*, 72, 189-199. doi:10.1016/j.chb.2016.12.049
- Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 8 U.S.C. § 1324a (1996).
- Indermaur, D., Roberts, L. D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology & Law*, 20(3), 315-328. doi:10.1080/13218719.2012.672275
- Internal Revenue Service. (2016). *Identity theft criminal investigation: Examples of identity theft investigations - Fiscal Year 2016*. Retrieved from <https://www.irs.gov/uac/identity-theft-criminal-investigation>
- Internal Revenue Service. (2017). *Identity theft criminal investigation: Examples of identity theft investigations - Fiscal Year 2017*. Retrieved from <https://www.irs.gov/uac/identity-theft-criminal-investigation>
- Jalaliyoon, N., Sahibuddin, S. & Taherdoost, H. (2011). Smart card security; technology and adoption. *International Journal of Security (IJS)*, 5(2), 74-84. Retrieved from <http://www.cscjournals.org/journals/IJS/>
- Jamieson, R., Land, L. P. W., Maurushat, A., Sarre, R., Steel, A., Stephens, G., & Winchester, D. (2012). Addressing identity crime in crime management information systems: Definitions, classification, and empirics. *Computer Law & Security Review*, 28, 381-395. doi:10.1016/j.clsr.2012.03.013
- Joyner, E. (2011). Enterprisewide fraud management: Detecting and preventing fraud in financial institutions (Paper No. 029-2011). Paper presented at the meeting of the SAS Global Forum, Cary, NC, 1-16. Retrieved from <http://support.sas.com/resources/papers/proceedings11/029-2011.pdf>
- Jung, K., & Lee, S. (2015). A systematic review of RFID applications and diffusion: Key areas and public policy issues. *Journal of Open Innovation: Technology, Market, and Complexity*, 1(9), 1-19. doi:10.1186/s40852-015-0010-z

- Kaelin, E., Kallischnigg, G., Vuillaume, G., & Weitkunat, R. (2010). Effectiveness of strategies to increase the validity of findings from association studies: Size vs. replication. *BMC Medical Research Methodology*, 10(47), 1-6. doi:10.1186/1471-2288-10-47
- Kamis, A., Ngugi, B., & Tremaine, M. (2011). Intention to use biometric systems. *E-Service Journal*, 7(3), 20-46. doi:10.2979/eservicej.7.3.20
- Karuppiah, M., & Saravanan, R. (2014). A secure remote user mutual authentication scheme using smart cards. *Journal of Information Security and Applications*, 19, 282-294. doi:10.1016/j.jisa.2014.09.006
- Kessler International. (2015). *Fake passports, driver's licenses, and police badges a click away*. Retrieved from <https://investigation.com/>
- Kihoro, J. M., Ngure, J. N., & Waititu, A. (2015). Principal component and principal axis factoring of factors associated with high population in urban areas: A case study of Juja and Thika, Kenya. *American Journal of Theoretical and Applied Statistics*, 4(4), 258-263. doi: 10.11648/j.ajtas.20150404.15
- Kim, S., Lee, S., & Wang, S. (2017). Motivation factors influencing intention of mobile sports apps use by applying the unified theory of acceptance and use of technology (UTAUT). *International Journal of Applied Sports Sciences*, 29(2), 115-127. doi:10.24985/ijass.2017.29.2.115
- Kindt, E. J. (2013). *Privacy and data protection issues of biometric applications: A comparative analysis* [Adobe Digital Editions version]. doi:10.1007/978-94-007-7522-0
- Kline, R. B. (2011). Computer tools. In D. A. Kenny, & T. D. Little (Eds.), *Principles and practice of structural equation modeling* (3rd ed.) (pp. 75-88). New York, NY: The Guilford Press.
- Kline, R. B. (2012). Assumptions of structural equation modeling. In R. Hoyle (Ed.), *Handbook of structural equation modeling* (pp. 111-125). New York: Guilford Press.
- Kline, R. B. (2013). Exploratory and confirmatory factor analysis. In Y. Petscher & C. Schatsschneider (Eds.), *Applied quantitative analysis in the social sciences* (pp. 171-207). New York, NY: Routledge.
- Kluwer, W. (Ed.). (2015). Tax briefing: Identity theft update; as identity theft grows, IRS and practitioners react. *Journal of Tax Practice & Procedure*, 17(5), 29-32. Retrieved from <https://www.cchgroup.com/store/products/>
- Kravitz, G. D. (2009). Real ID: The devil you don't know. *Harvard Law & Policy Review*, 3(2), 431-446. Retrieved from www.hls.harvard.edu

- Krickett, J. D. (2015). The high cost of missing the EMV chip card switch. *Podiatry Management*, 34(7), 59-64. Retrieved from <http://www.podiatrym.com/>
- Kühne, S., & Krasmann, S. (2014). "My fingerprint on Osama's cup." On objectivity and the role of the fictive regarding the acceptance of a biometric technology. *Surveillance & Society* 12(1), 1-14. Retrieved from <http://www.surveillance-and-society.org/>
- Kunick, J. M., & Posner, N. B. (2011). Following the red flag rules to detect and prevent identity theft. *Information Management Journal*, 45(3), 25-28. Retrieved from <http://content.arma.org/IMM/online/InformationManagement.aspx>
- Kwon, T., Na, S., & Shin, S. (2014). Covert attentional shoulder surfing: Human adversaries are more powerful than expected. *IEEE Transactions on Systems, Man, And Cybernetics: Systems*, 44(6), 716-727. doi:10.1109/TSMC.2013.2270227
- Laas-Mikko, K., & Sutrop, M. (2012). How do violations of privacy and moral autonomy threaten the basis of our democracy? *TRAMES: A Journal of The Humanities & Social Sciences*, 16(4), 369-381. doi:10.3176/tr.2012.4.05
- Lackey, N. R., Pett, M. A., & Sullivan, J. J. (2003). *Making sense of factor analysis: The use of factor analysis for instrument development in health care research*. Thousand Oaks, CA: SAGE Publications, Inc.
- Lawrence, B. M. (2016). iPad acceptance by English learners in Saudi Arabia. *English Language Teaching*, 9(12), 34-46. doi:10.5539/elt.v9n12p34
- Lederer, A., & Wu, J. (2009). A meta-analysis of the role of environment-based voluntariness in information technology acceptance. *MIS Quarterly*, 33(2), 419-432. Retrieved from <http://www.misq.org/>
- Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Upper Saddle River, NJ: Pearson Education, Inc.
- Leskinen, E., & Niemelä-Nyrhinen, J. (2014). Multicollinearity in marketing models: Notes on the application of ridge trace estimation in structural equation modelling. *The Electronic Journal of Business Research Methods*, 12(1), 3-15. Retrieved from <http://www.ejbrm.com/main.html>
- Levenson, A. (2014). *Employee surveys that work: Improving design, use, and organizational impact*. San Francisco, CA: Berrett-Koehler Publishers, Inc.
- Lewis, P., Saunders, M. N. K., & Thornhill, A. (2015). *Research methods for business students* (7th ed.). Essex, England: Pearson Education Limited.

- Li, L., Lu, Y., Yang, Y., & Peng, H. (2015a). A biometrics and smart cards-based authentication scheme for multi-server environments. *Security and Communication Networks*, 8, 3219-3228. doi:10.1002/sec.1246
- Li, L., Lu, Y., Yang, X., & Yang, Y. (2015b). Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. *PLoS ONE*, 10(5), 1-13. doi:10.1371/journal.pone.0126323
- Liu, M., & Wronski, L. (2016). Calibrating cross-national panel surveys. In *Proceedings of the International Conference on Survey Methods in Multinational, Multiregional and Multicultural Contexts (3MC)*, Chicago (pp. 1-16). Retrieved from https://www.csdiworkshop.org/images/2016_3MC_Presentations/Wronski_Calibrating-Cross-National-Panel-Surveys.pdf
- Loo, W., Yeow, P. H., & Yuen, Y. (2013). Ergonomics issues in national identity card for homeland security. *Applied Ergonomics*, 44(5), 719-729. doi:10.1016/j.apergo.2012.04.017
- Lott, D. (2015). *Improving customer authentication*. Federal Reserve Bank of Atlanta. Retrieved from https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/improving-customer-authentication.pdf
- Louw, T., Madigan, R., Merat, N., Schieben, A., & Wilbrink, M. (2017). What influences the decision to use automated public transport? Using UTAUT to understand public acceptance of automated road transport systems. *Transportation Research Part F: Traffic Psychology and Behaviour*, 50, 55-64. doi:10.1016/j.trf.2017.07.007
- Lyon, D. (2010). National IDs in a global world: Surveillance, security, and citizenship. *Case Western Reserve Journal of International Law*, 42(3), 607-623. Retrieved from <http://law.case.edu/journals/JIL/>
- Maniff, J. L., & Sullivan, R. J. (2016). Data Breach notification laws. *Economic Review*, 101(1), 65-85. Retrieved from <https://www.kansascityfed.org/>
- Mansfeld, Y., & Pizam, A. (Eds.). (2006). *Tourism, security and safety: From theory to practice*. Jordan Hill, England: Elsevier.
- Marchini, K., Miller, S., & Pascual, A. (2017). *2017 identity fraud: Securing the connected life*. Javelin Strategy & Research. Retrieved from <https://www.javelinstrategy.com/coverage-area/2017-identity-fraud>
- Marechal, S. (2008). Advances in password cracking. *Journal of Computer Virology*, 4, 73-81. doi:10.1007/s11416-007-0064-y

- Martin, A., Wallace, C., & Walton, J. R. (2015). *Best practices for the implementation of the Real ID Act*. University of Kentucky, College of Engineering, Kentucky Transportation Center. doi:10.13023/KTC.RR.2015.23
- Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34, 1-13. doi:10.1016/j.ijinfomgt.2013.06.002
- Mavroudi, E., & Warren, A. (2011). Managing surveillance? The impact of biometric residence permits on UK migrants. *Journal of Ethnic and Migration Studies*, 37(9), 1495-1511. doi:10.1080/1369183X.2011.623624
- Maydeu-Olivares, A. (2017). Maximum likelihood estimation of structural equation models for continuous data: Standard errors and goodness of fit. *Structural Equation Modeling*, 24(3), 383-394. doi:10.1080/10705511.2016.1269606
- McGrath, K. (2016). Identity verification and societal challenges: Explaining the gap between service provision and development outcomes. *MIS Quarterly*, 40(2), 485-500. Retrieved from <http://www.misq.org/>
- McGuire, J., & Scott, S. (2017). Using diffusion of innovation theory to promote universally designed college instruction. *International Journal of Teaching and Learning in Higher Education*, 29(1), 119-128. Retrieved from <http://www.isetl.org/ijtlhe/>
- Meagher, K. M. (2015). Seeking context for the duty to rescue: Contractualism and trust in research institutions. *American Journal of Bioethics*, 15(2), 18-20. doi:10.1080/15265161.2014.990170
- Medicare Common Access Card Act of 2015, 4151. H.R. 1871 S. § 2 (2015).
- Miles, J. (2003). A framework for power analysis using a structural equation modelling procedure. *BioMed Central (BMC) Medical Research Methodology*, 3(27), 1-11. doi:10.1186/1471-2288-3-27
- Miller, J. A. (2016). Constitutional law--The Real Id Act: Violating Massachusetts residents' right to travel and the tenth amendment. *Western New England Law Review*, 38(1), 127-161. Retrieved from <http://www1.wne.edu/law/law-review/index.cfm>
- Miller, J. J., & Moore, S. (1995). A national ID system: Big brother's solution to illegal immigration. *Cato Policy Analysis*, 237. Retrieved from <http://www.cato.org/pubs/pas/pa237.html>

- Miltgen, C. L., Oliveira, T., & Popović, A. (2013). Determinants of end-user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context. *Decision Support Systems*, 56, 103-114. doi:10.1016/j.dss.2013.05.010
- Moeser, G., & Moryson, H. (2016). Consumer adoption of cloud computing services in Germany: Investigation of moderating effects by applying an UTAUT model. *International Journal of Marketing Studies*, 8(1), 14-32. doi:10.5539/ijms.v8n1p14
- Mol, C. V. (2017) Improving web survey efficiency: the impact of an extra reminder and reminder content on web survey response. *International Journal of Social Research Methodology*, 20(4), 317-327. doi:10.1080/13645579.2016.1185255
- Montazemi, A. R., & Qahri-Saremi, H. (2015). Factors affecting adoption of online banking: A meta-analytic structural equation modeling study. *Information & Management*, 52(2), 210-226. doi:10.1016/j.im.2014.11.002
- Morosan, C. (2012a). Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *Journal of Hospitality and Tourism Research*, 36(1), 52-84. doi:10.1177/1096348010380601
- Morosan, C. (2012b). Voluntary steps toward air travel security: An examination of travelers' attitudes and intentions to use biometric systems. *Journal of Travel Research*, 51(4), 436. doi:10.1177/0047287511418368
- Morosan, C. (2016). An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports. *Journal of Air Transport Management*, 55, 120-128. doi:10.1016/j.jairtraman.2016.05.005
- Mtebe, J. S., & Raisamo, R. (2014). Investigating students' behavioural intention to adopt and use mobile learning in higher education in East Africa. *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 10(3), 4-20. Retrieved from <http://ijedict.dec.uwi.edu/>
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. Washington, DC: U.S. Government Printing Office.
- National Conference of State Legislatures. (2017a). *Child support 101.2: Locating a noncustodial parent*. Retrieved from <http://www.ncsl.org/research/human-services/enforcement-locating-a-noncustodial-parent.aspx>
- National Conference of State Legislatures. (2017b). *Identity theft*. Retrieved from <http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx>

- National Immigration Law Center. (2016). *The Real ID Act: Questions and answers*. Retrieved from <https://www.nilc.org/wp-content/uploads/2015/11/REAL-ID-Act-Q-and-A.pdf>
- New York State Department of Motor Vehicles. (2017). *Proof requirements for a permit, license or non-driver ID*. Retrieved from <https://dmv.ny.gov/driver-license/prove-identity-age-permitlicense>
- Nugroho, Y. (2011). Opening the black box: The adoption of innovations in the voluntary sector—the case of Indonesian civil society organizations. *Research Policy*, 40(5), 761-777. doi:10.1016/j.respol.2011.03.002
- O’Leary A. O. (Ed.). (2014). *Immigrants in the United States: An encyclopedia of their experience* (Vol. I: A-J). Santa Barbara, CA: ABC-CLIO, LLC.
- Pallant, J. (2016). *SPSS survival manual: A step by step guide to data analysis using SPSS* (6th ed.). Sydney, Australia: Allen & Unwin
- Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, 3(1), 1-7. doi:10.15577/jmt.2016.03.01.1
- Po-liang, C., & Yung-hua, K. (2016). Identity laws and privacy protection in a modern state: The legal history concerning personal information in Taiwan (1895-2015). *Washington International Law Journal*, 25(2), 223-266. Retrieved from <https://www.law.washington.edu/winlj/>
- Pocs, M. (2013). Legally compatible design of future biometric systems for crime prevention. *Innovation: The European Journal of Social Science Research*, 26(1-2), 36-56. doi:10.1080/13511610.2013.747659
- Polit, D. F. (2010), *Statistics and data analysis for nursing research* (2nd ed.). Upper Saddle River, NJ: Pearson.
- Rahman, W., Rasli, A., & Shah, F. A. (2015). Use of structural equation modeling in social science research. *Asian Social Science*, 11(4), 371-377. doi:10.5539/ass.v11n4p371
- Rajankar, S. O., & Shaikh, F. A. (2016). Biometric authentication system using RPI. *International Journal of Engineering Sciences & Research Technology*, 5(4), 839-844. Retrieved from <http://www.ijesrt.com/>
- Ramanathan, U. (2015). Considering social implications of biometric registration: A database intended for every citizen in India [Commentary]. *IEEE Technology & Society Magazine*, 34(1), 10. doi:10.1109/MTS.2015.2396113

- Randall, B. (2014). Death certification: A primer. Part I—An introduction to the death certificate. *The Journal of the South Dakota State Medical Association*, 67(5), 196-199. Retrieved from <https://www.sdsma.org/>
- Real ID Act of 2005, 109-113 §201-202, 119 Stat. 312-314 (2005).
- Real ID Act of 2005 proceedings and debates, 109 Cong. 1908-1926 (2005).
- Renaud, T. L. (2016, March 26). *Recommendation next generation secure identification document project - permanent resident card and employment authorization document card designs* [Memorandum]. Washington, DC: U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services. Retrieved from https://www.uscis.gov/sites/default/files/files/natedocuments/Next_Generation_Secure_Identification_Document_Project.pdf
- Reznik, M. (2013). Identity theft on social networking sites: Developing issues of Internet impersonation. *Touro Law Review*, 29(2), 455-483. Retrieved from <https://www.tourolaw.edu/lawreview/>
- Rogers, E. M. (1962). *Diffusion of innovations* (1st ed.). New York, NY: Free Press
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). New York, NY: Free Press.
- Salim, S. A., Sawanga, S., & Sun Y. (2014). It's not only what I think but what they think! The moderating effect of social norms. *Computers & Education*, 76, 182-189. doi:10.1016/j.compedu.2014.03.017
- Seyal, A. H., & Turner, R. (2013). A study of executives' use of biometrics: An application of theory of planned behaviour. *Behaviour & Information Technology*, 32(12), 1242-1256. doi:10.1080/0144929X.2012.659217
- Shaqrah A. (2015). Explain the behavior intention to use e-learning technologies: A unified theory of acceptance and use of technology perspective. *International Journal of Web-Based Learning and Teaching Technologies*, 10(4), 19-32. doi:10.4018/IJWLTT.2015100102
- Soares, E. (2011, January). Brazil: New national ID card launched. *Library of Congress*. Retrieved from http://www.loc.gov/lawweb/servlet/lloc_news?disp3_1205402458_text
- Social Security Administration. (n.d.). *New or replacement social security number and card*. Retrieved from <https://www.ssa.gov/ssnumber/>
- Social Security Identity Theft Prevention Act, 5405 H.R. § 2 (2008).

- Šorgo, A., & Šumak, B. (2016). The acceptance and use of interactive whiteboards among teachers: Differences in UTAUT determinants between pre- and post-adopters. *Computers in Human Behavior*, 64, 602-620. doi:10.1016/j.chb.2016.07.037
- Spil, I. T. A. M., Yan, J., Yu, P., & Zhang, X. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer e-health innovations: A case study in a primary care clinic. *BMC Health Services Research*, 15(71), 1-15. doi:10.1186/s12913-015-0726-2
- Sullivan, G. M. (2011). A primer on the validity of assessment instruments. *Journal of Graduate Medical Education*, 3(2), 119-120. doi:10.4300/JGME-D-11-00075.1
- Sullivan, R. J. (2013). The U.S. adoption of computer-chip payment cards: Implications for payment fraud. *Economic Review*, (1), 59-87. Retrieved from <https://www.aeaweb.org/journals/aer>
- SurveyMonkey. (2016). *SurveyMonkey Contribute privacy statement*. Retrieved from <https://contribute.surveymonkey.com/privacy>
- Sweta. (2015). Smart card and its applications. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(7), 1158-1160. Retrieved from <http://www.ijarcsse.com/>
- Taber, K. S. (2017). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, 1-24. doi:10.1007/s11165-016-9602-2
- Tao, Y. H., Wu, Y. L., & Yang, P. C. (2007). Using UTAUT to explore the behavior of 3G mobile communication users. In *Proceedings of the International Conference on Industrial Engineering and Engineering Management (IEEM)*, Singapore (pp. 199-203). doi:10.1109/IEEM.2007.4419179
- Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), 144-176. doi:10.1287/isre.6.2.144
- Teo, T. (2011). Factors influencing teachers' intention to use technology: Model development and test. *Computers & Education*, 57(4), 2432-2440. doi:10.1016/j.compedu.2011.06.008
- Thiessen, P. R. (2008). The Real ID Act and biometric technology: A nightmare for citizens and the states that have to implement it. *Journal on Telecommunications & High Technology Law*, 6(2), 483-508. Retrieved from <http://www.jthtl.org/>
- Thong, J. Y. L., Venkatesh, V., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology.

- Management Information Systems Quarterly*, 36(1), 157-178. Retrieved from <http://www.misq.org/>
- TripAdvisor. (2016). *The top 25 destinations – United States*. Retrieved from <https://www.tripadvisor.com/TravelersChoice-Destinations-cTop-g191>
- University of California, Los Angeles Institute for Digital Research and Education. (2016). *G*Power data analysis examples*. Retrieved from <http://www.ats.ucla.edu/stat/gpower/indepsamps.htm>
- U.S. Census Bureau. (2016). *Population estimates by age (18+): July 1, 2016*. Retrieved from <https://www.census.gov/data/tables/2016/demo/popest/nation-detail.html>
- U.S. Citizenship and Immigration Services. (2016). Petition for a spouse. *Adjudicator's Field Manual*. Retrieved from <https://www.uscis.gov/laws/immigration-handbooks-manuals-and-guidance>
- U.S. Citizenship and Immigration Services. (2017). *Green card*. Retrieved from <https://www.uscis.gov/greencard>
- U.S. Citizenship and Immigration Services. (2017, April). *USCIS will issue redesigned green cards and employment authorization documents*. Retrieved from <https://www.uscis.gov/news-releases>
- U.S. Department of Defense. (2014). *DoD identification (ID) cards: ID card life-cycle* (Department of Defense Manual 1000.13, Vol. 1). Retrieved from http://www.cac.mil/docs/DODM-1000.13_vol1.pdf
- U.S. Department of Homeland Security. (2015). *Enhanced drivers licenses: What are they?* Retrieved from <https://www.dhs.gov/enhanced-drivers-licenses-what-are-they>
- U.S. Department of Homeland Security. (2016a). *REAL ID frequently asked questions for the public*. Retrieved from <https://www.dhs.gov/real-id-public-faqs>
- U.S. Department of Homeland Security. (2016b). *TSA to notify travelers of upcoming 2018 Real ID airport enforcement - signs at airports to inform travelers of ID requirements at security checkpoints*. Retrieved from <https://www.dhs.gov/news/>
- U.S. Department of Homeland Security. (2017). *Current status of states/territories*. Retrieved from <https://www.dhs.gov/current-status-states-territories>
- U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. (2015). *Victims of identity theft, 2014* (NCJ Publication No. 248991). Retrieved from <https://www.bjs.gov/content/pub/pdf/vit14.pdf>

- U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime. (2010). *Identity theft and financial fraud: Federal identity theft laws* (National Criminal Justice Publication No. 230590). Retrieved from https://ojp.gov/ovc/pubs/ID_theft/idtheftlaws.html
- U.S. Government Accountability Office. (2016, January). *Health care fraud: Information on most common schemes and the likely effect of smart cards* (GAO-16-216). Retrieved from <http://www.gao.gov/products/GAO-16-216>
- Vogt, W. P. (2007). *Quantitative research methods for professionals*. Boston, MA: Pearson/Allyn and Bacon.
- Walker, E. M. (2015). Biometric boom: How the private sector commodifies human characteristics. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 25(3), 831-867. Retrieved from <http://ir.lawnet.fordham.edu/iplj/>
- Weng, Y. C., Wu, M. Y., & Yu, P. Y. (2012). A study on user behavior for I Pass by UTAUT: Using Taiwan's MRT as an example. *Asia Pacific Management Review*, 17(1), 91-111. Retrieved from <http://apmr.management.ncku.edu.tw/>
- Wiehl, C. (2012). Reliance on identification to secure the blessings of liberty and property. *UMKC Law Review*, 81(2), 509-538. Retrieved from <https://umkcclawreview.org/>
- Williams, S. G. (2012). The ethics of Internet research. *Online Journal of Nursing Informatics (OJNI)*, 16(2), 1-12. Retrieved from <http://ojni.org/>
- Yücel, E. (2013). Effectiveness of red flags in detecting fraudulent financial reporting: An application in Turkey. *Journal of Accounting & Finance*, 60, 139-158. Retrieved from <http://www.na-businesspress.com/jafopen.html>
- Zureik, E. (2010). Cross-cultural study of surveillance and privacy theoretical and empirical observations. In Y. E. Chan, D. Lyon, E. Smith, L. H. Stalker, & E. Zureik (Eds.), *Surveillance, privacy, and the globalization of personal information: International comparisons* (pp. 348-360). Montreal, Canada: McGill-Queen's University Press.

Appendices

Appendix A: Research Questionnaire

This survey questionnaire examines the U.S. public's perceptions of a combined biometric and smart card technology (CBIOSCT) in existing forms of personal identification.

The purpose of this survey is to assess the U.S. public's intention to use a CBIOSCT in existing forms of personal identification for identity theft and identity fraud prevention. Your collaboration in completing this questionnaire as accurately as possible is much appreciated. All information provided will be kept confidential.

Section 1. Demographic Information

Please circle the number which best represents your personal description.

1. City of current residence^a

- | | |
|-----------------------|-------------------------------------|
| 1. New York, New York | 2. Washington, District of Columbia |
| 3. Orlando, Florida | 4. Charleston, South Carolina |
| 5. Las Vegas, Nevada | 6. San Francisco, California |

2. Are you legally eligible for a driver's license or a state identification card?

- 1 Yes 2. No

3. Age group

- | | |
|------------------------|-------------------------------|
| 1 18-24 years old | 2 25-45 years old |
| 3 46-63 years old | 4 64 years old and above |

4. Gender

- 1 Male 2 Female

5. Highest level of education

- | | |
|--|---|
| 1 High school degree or equivalent | 2 Bachelor of Science/Arts or equivalent |
| 3 Master's degree or equivalent | 4 Doctoral degree or equivalent |
| 5 Medical or law degree or equivalent | 6 Other (please state) |

6. Annual household income

- | | |
|------------------------------|------------------------------|
| 1 \$50,000 or less | 2 \$50,001 - \$100,000 |
| 3 \$100,001 - \$150,000 | 3 \$150,001 - \$200,000 |
| 4 \$200,001 or more | |

^a Current residence: refers to the place where you live.

Section 2: Factors affecting intention to use CBIOSCT

Please circle the appropriate number that indicates the response that best describes your agreement or disagreement with the factors that affect your intention to use a CBIOSCT in existing forms of personal identification for identity theft and identity fraud prevention.

Scale:

1 = strongly disagree, 2 = disagree, 3 = neither agree nor disagree, 4 = agree, 5 = strongly agree

1. Performance expectancy (PE)

Using CBIOSCT will protect me against identity theft (PE1).

1 2 3 4 5

Using CBIOSCT will enhance the reliability of my personal data thus protect me against identity fraud (PE2).

1 2 3 4 5

Using CBIOSCT allows for an effective identity verification and authentication process (PE3).

1 2 3 4 5

2. Perceived credibility (PC): Safety and privacy

CBIOSCT is difficult to be forged by criminals (PC1).

1 2 3 4 5

Using CBIOSCT is secure (PC2).

1 2 3 4 5

CBIOSCT limits unauthorized access to users' personal information (PC3).

1 2 3 4 5

3. Social influence (SI)

People who are important^b to me influence my intention to use the CBIOSCT (SI1).

1 2 3 4 5

People I know who are using CBIOSCT at their workplace influence my intention to use CBIOSCT (SI2).

1 2 3 4 5

The United States government's encouragement influences my intention to use the CBIOSCT (SI3).

1 2 3 4 5

4. Facilitating conditions (FC)

CBIOSCT infrastructure is available in government and private sectors for identity authentication and fraud risk detection (FC1).

1 2 3 4 5

A customer service contact center is available to answer CBIOSCT users' inquiries (FC2)

1 2 3 4 5

Current driver's licenses and state ID cards embedded technology^c are likely to be phased out soon (FC3).

1 2 3 4 5

^b People who are important: Refers to family members, relatives, friends, or other people close to you.

^c Current driver's licenses and state ID cards embedded technology: refers to the hardware and software within these forms of identification

5. Attitude (Att)

The use of a CBIOSCT in existing forms of personal identification in the U.S. to combat identity theft and identity fraud is a good idea (Att1)

1 2 3 4 5

I feel that the use of CBIOSCT for identity theft and identity fraud prevention is beneficial (Att2).

1 2 3 4 5

The use of CBIOSCT would enhance our standard of living^d (Att3).

1 2 3 4 5

Section 3: Intention to use the CBIOSCT

Please circle the appropriate number that indicate the response that best describes your agreement or disagreement on the factors that affect your intention to use a CBIOSCT in existing forms of personal identification in the United States for identity theft and identity fraud prevention.

Scale:

1 = strongly disagree, 2 = disagree, 3 = neither agree nor disagree, 4 = agree, 5 = strongly agree

Behavioral Intention (BI) to use CBIOSCT

I intend to use CBIOSCT for identification purposes (BI1)

1 2 3 4 5

I predict I would use CBIOSCT for identity theft and fraud prevention (BI2)

1 2 3 4 5

I plan to continue to use CBIOSCT in the future for identity theft and fraud prevention (BI3)

1 2 3 4 5

End of Questionnaire

Please check to ensure that you have not missed any questions.

I sincerely appreciate your time and collaboration. Thank you.

^d Standard of living: refers to the level of comfort and safety in everyday life enjoyed by a person.

Appendix B: Site Permission



SurveyMonkey Inc.
www.surveymonkey.com

For questions, visit our Help Center
help.surveymonkey.com

Re: Permission to Conduct Research Using SurveyMonkey

To whom it may concern:

This letter is being produced in response to a request by a student at your institution who wishes to conduct a survey using SurveyMonkey in order to support their research. The student has indicated that they require a letter from SurveyMonkey granting them permission to do this. Please accept this letter as evidence of such permission. Students are permitted to conduct research via the SurveyMonkey platform provided that they abide by our Terms of Use, a copy of which is available on our website.

SurveyMonkey is a self-serve survey platform on which our users can, by themselves, create, deploy and analyze surveys through an online interface. We have users in many different industries who use surveys for many different purposes. One of our most common use cases is students and other types of researchers using our online tools to conduct academic research.

If you have any questions about this letter, please contact us through our Help Center at help.surveymonkey.com.

Sincerely,

SurveyMonkey Inc.



Appendix C: Survey Introductory Letter

My name is Silvia Tovar-Rivera. I am a doctoral student at Northcentral University. As part of my PhD investigation, I am conducting a research study on the issues surrounding the United States (U.S.) public's intention to adopt a Combined Biometric and Smart Card Technology (CBIOSCT) as an alternative to current forms of identification for identity theft and identity fraud prevention. I am completing this investigation as part of my doctoral degree and invite you to participate in a web-based online survey. It will take you no more than 15 minutes to complete the survey.

You may participate in this study if you:

1. Currently live in the U.S. within the following cities New York City, New York; Washington, District of Columbia; Orlando, Florida; Charleston, South Carolina; Las Vegas, Nevada; and San Francisco, California.
2. Are 18 years of age and older.
3. Are eligible to apply for a driver's license or a state identification card.

I would appreciate your participation in this study. All of your responses will be confidential and anonymous. Your answers will be used only as part of the statistics for the study. No incentives are offered and your decision to participate in this study is voluntary. You may choose to leave the study at any time or refuse to answer any questions that may be asked during the study. If you have any questions about the survey questions, you can contact me at S.TovarRivera1212@o365.ncu.edu.

Please click on the provided link, carefully read through the consent form, and answer the survey questions. Thank you for your time and cooperation.

Sincerely,

Silvia Tovar-Rivera
Doctoral Candidate, School of Business and Technology Management
Northcentral University
S.TovarRivera1212@o365.ncu.edu

Appendix D: Informed Consent Form

Dear participant:

My name is Silvia Tovar-Rivera and I am a doctoral student at Northcentral University. I am conducting a research study on the issues surrounding the United States (U.S.) public's intention to adopt a Combined Biometric and Smart Card Technology (CBIOSCT) as an alternative to current forms of identification for identity theft and identity fraud prevention. I am completing this research as part of my doctoral degree and invite you to participate.

Activities:

If you participate in this research, you will be asked to:

1. Carefully read through the survey introductory letter and the informed consent form (4 minutes)
2. Click on the provided link and answer the questionnaire (11 minutes)

Eligibility:

You are eligible to participate in this research if you:

1. Currently live in the U.S. within the cities listed in Section 1, Question 1 of the survey.
2. Are 18 years of age and older.
3. Are eligible for a driver's license or a state identification card.

You are not eligible to participate in this research if you:

1. Do not live in the U.S. within the cities listed in Section 1, Question 1 of the survey.
2. Are under 18 years of age.
3. Are not eligible for a driver's license or a state identification card.

I hope to include 600 people in this research.

Risks:

There are minimal risks in this study. Some possible risks include: psychological stress of filling out a survey about your viewpoints, which are not greater, than those ordinarily encountered in daily life.

To decrease the impact of these risks, you can skip any question, or end your participation at any time.

Benefits:

If you decide to participate, there are no direct benefits to you. The potential benefits to others are: The study results will provide scientific interest that may eventually highlight promising directions for future investigations.

Confidentiality:

The information you provide will be kept confidential to the extent allowable by law. You will enter your data into the SurveyMonkey website. Survey Monkey is a secure, confidential website, you may check their privacy policy at <https://www.surveymonkey.com/mp/policy/>. A further step I will take to keep your identity confidential is an anonymous survey with no names collected.

The people who will have access to your information are: myself, my dissertation chair, and my dissertation committee. The Institutional Review Board may also review my research and view your information.

I will secure your information with these steps: Locking the computer file with a password and locking the hard drive in a file cabinet.

I will keep your data for 7 years. Then, I will delete electronic data and destroy paper data.

Contact Information:

If you have questions for me, you can contact me at: S.TovarRivera1212@o365.ncu.edu

My dissertation chair's name is Dr. Garrett Smiley. He works at Northcentral University and is supervising me on the research. You can contact him at: gsmiley@ncu.edu.

If you have questions about your rights in the research, or if a problem has occurred, or if you are injured during your participation, please contact the Institutional Review Board at: irb@ncu.edu or 1-888-327-2877 ext 8014.

Voluntary Participation:

Your participation is voluntary. If you decide not to participate, or if you stop participation after you start, there will be no penalty to you. You will not lose any benefit to which you are otherwise entitled.

Signature:

Participant, if you agree to the above terms, by clicking Yes, you consent that you are willing to answer the question in this survey. Also, if you would like to have your name linked to the survey, please type your name at the end of this consent form. Providing your name is optional. If you click No or exit the survey, then you do not agree to participate, and you will not be moving on to complete the Survey, I sincerely thank you for your time.

Participant Printed Name

Date

Thank you,

Silvia Tovar-Rivera
Northcentral University
S.TovarRivera1212@o365.ncu.edu

Appendix E: G*power Estimated Sample Size

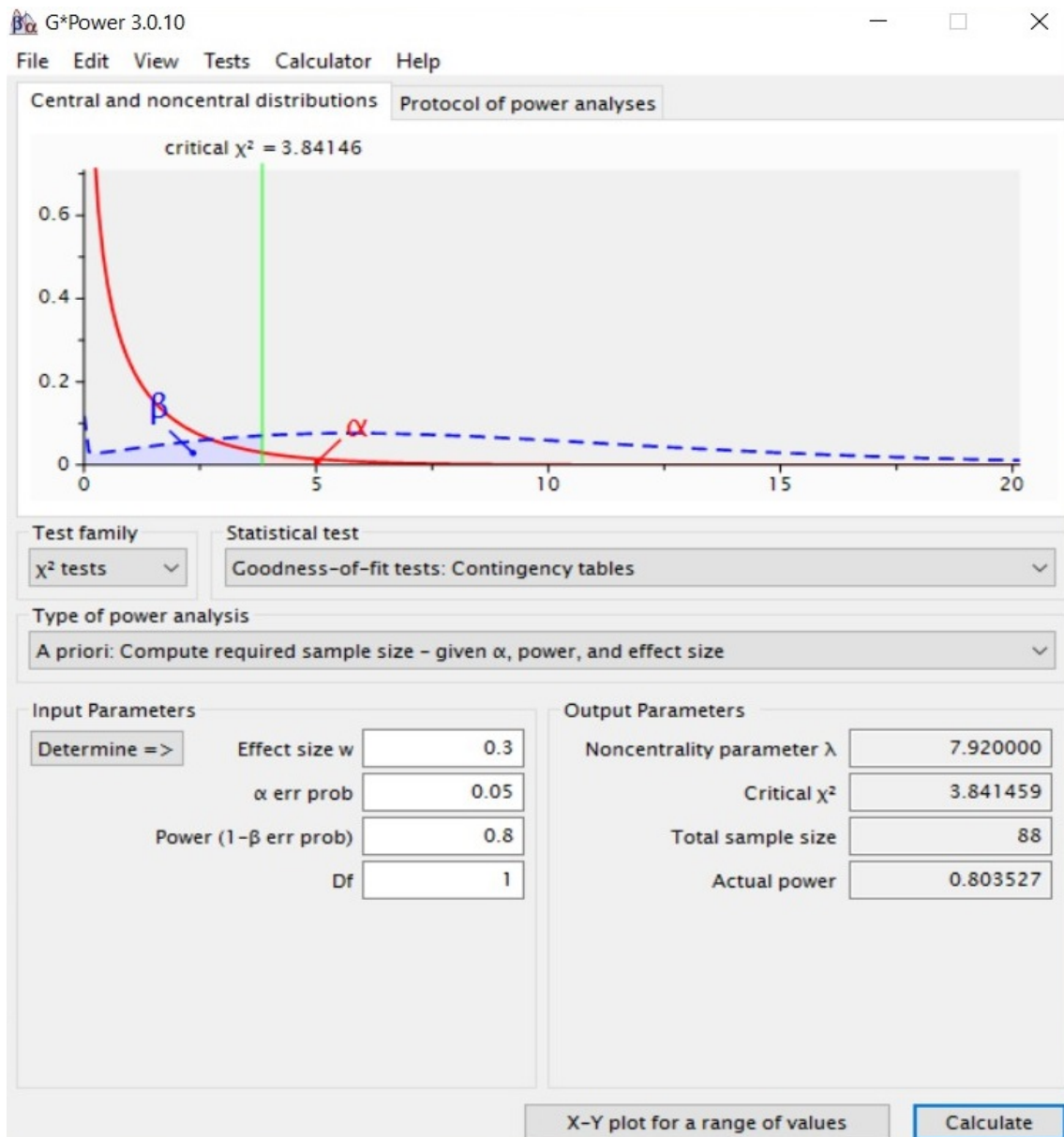


Figure E1. Chi-square (X^2) test of goodness of fit.

Note. The window produces the desired result along with, in descending order, the noncentrality parameter λ , the critical X^2 , the total sample size, and the test's actual power. In addition, a graphical representation of the test is shown with the sampling distribution appearing as a dotted blue line, the population distribution represented by a solid red line, a red shaded area delineating the probability of a type 1 error, a blue area for the type 2 error, and a green line demarcating the critical point X^2 (University of California, Los Angeles Institute for Digital Research and Education, 2016).

Appendix F: Permission to Use Survey Instruments – Loo et al.

3/29/2017

Re: Permission to adopt and modify survey questions - Silvia, Tovar-Rivera

From: Paul Yeow <paul.yeow@monash.edu>
Sent: Tuesday, March 28, 2017 11:23:11 AM
To: Silvia, Tovar-Rivera
Cc: weehong@iputra.edu.my; pyhp@yahoo.com; yeeven2388@gmail.com
Subject: Re: Permission to adopt and modify survey questions from your study entitled: Ergonomics issues in national identity card for homeland security.

Dear Silva,

We are happy to give you our consent. Let me know if you do need any help in your research.

Regards,
 Paul Yeow
 Associate Professor,
 Monash University

 This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited

On 28 March 2017 at 21:39, Silvia, Tovar-Rivera <S.TovarRivera1212@email.ncu.edu> wrote:

Dr. Loo, Dr. Yeow, and Dr. Yuen:

I am currently pursuing a PhD in Business Administration with computer and information security specialty from Northcentral University, Prescott, Arizona. To fulfill the requirements of this degree, I am conducting a quantitative research focused on examining the ergonomics issues surrounding the United States (U.S.) public's intention to adopt a Combined Biometric and Smart Card Technology (CBIOSCT) as an alternative to current forms of identification for identity theft and identity fraud prevention. For my research, I need to compile a survey instrument that can be administered online. Therefore, I would like to request your permission to adopt and modify survey questions from your study entitled: Ergonomics issues in national identity card for homeland security.

I hope to use your research as one of the basis for my dissertation to apply the theory to a new situation in the context of the United States, to determine the generalizability of findings, modifying some of the variables in an try and duplicate these findings in the context of the United States. Also, I changed the theory slightly to add the attitude construct and remove the anxiety variable to determine if this new variable plays any role in my research study.

I look forward to receiving your consent to use and modify the instrument for my dissertation.

I will be sure to provide adequate reference to your work in my dissertation.

Please contact me at: S.TovarRivera1212@email.ncu.edu

Thank you,

Sincerely,

Silvia Tovar-Rivera
Doctoral Candidate
Northcentral University, AZ
USA

Appendix G: Permission to Use Survey Instruments – Dr. Morosan

3/29/2017

Re: Permission to adopt and modify survey questions ... - Silvia, Tovar-Rivera

Re: Permission to adopt and modify survey questions from your study entitled: An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports

Silvia, Tovar-Rivera

Wed 3/29/2017 2:28 PM

To: Morosan, Cristian <cmorosan@Central.UH.EDU>;

Dr. Morosan,

Thank you for your prompt response. I greatly appreciate your consent and good wishes. Also, thank you for your kind offer of help, I will let you know if I may have any questions about your study.

Once again, thank you so much for your permission.

Sincerely,

Silvia Tovar-Rivera
Doctoral Candidate
Northcentral University, AZ
USA

From: Morosan, Cristian <cmorosan@Central.UH.EDU>

Sent: Wednesday, March 29, 2017 12:01:06 PM

To: Silvia, Tovar-Rivera

Subject: Re: Permission to adopt and modify survey questions from your study entitled: An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports

Hi Silvia,

Your topic is very interesting. You can modify my instrument as you see fit. Best of luck with your dissertation and please let me know if you need any help.

Sincerely,
Cristian Morosan

Sent from my iPad

On Mar 29, 2017, at 5:29 PM, Silvia, Tovar-Rivera <S.TovarRivera1212@email.ncu.edu> wrote:

Dr. Morosan:

I am currently pursuing a PhD in Business Administration with computer and information security specialty from Northcentral University, Prescott, Arizona. To fulfill the requirements of this degree, I am conducting a quantitative research focused on examining the ergonomics issues surrounding the United States (U.S.) public's intention to adopt a Combined Biometric and Smart Card Technology

(CBIOSCT) as an alternative to current forms of identification for identity theft and identity fraud prevention. For my research, I need to compile a survey instrument that can be administered online. Therefore, I would like to request your permission to adopt and modify demographic survey questions from your study entitled: An empirical examination of U.S. travelers' intentions to use biometric e-gates in airports. I hope to use your demographic questions to produce a profile of respondents.

I look forward to receiving your consent to use and modify the instrument for my dissertation.

I will be sure to provide adequate reference to your work in my dissertation.

Please contact me at: S.TovarRivera1212@email.ncu.edu

Thank you,

Sincerely,

Silvia Tovar-Rivera
Doctoral Candidate
Northcentral University, AZ
USA

Appendix H: Permission to Use Survey Instruments – Bush et al. (2014)

3/29/2017

Re: Permission to adopt and modify survey questions ... - Silvia, Tovar-Rivera

Re: Permission to adopt and modify survey questions from your study entitled: Incorporating UTAUT predictors for understanding home care patients' and clinician's acceptance of healthcare telemedicine equipment

Silvia, Tovar-Rivera

Wed 3/29/2017 8:04 PM

Sent Items

To: Anne Kohnke <akohnke@ltu.edu>;

Dr. Kohnke,

Thank you for your prompt response, and for sending me a copy of your questionnaire. Also, I greatly appreciate your consent and good wishes. I will be sure to provide adequate reference to your work in my dissertation.

Once again, thank you so much for your permission.

Sincerely,

Silvia Tovar-Rivera
Doctoral Candidate
Northcentral University, AZ
USA

From: Anne Kohnke <akohnke@ltu.edu>

Sent: Wednesday, March 29, 2017 3:35:01 PM

To: Silvia, Tovar-Rivera

Subject: RE: Permission to adopt and modify survey questions from your study entitled: Incorporating UTAUT predictors for understanding home care patients' and clinician's acceptance of healthcare telemedicine equipment

Hello Silvia,

Attached is the survey I created for this study and you have permission to use this instrument with citation. I wish you all the best!

Kindest regards,
Anne Kohnke, PhD
Assistant Professor of IT
College of Management
Lawrence Technological University
21000 West Ten Mile Road
Southfield, MI 48075
Buell Building, M320
LTU Office: 248.204.3085
Home Office: 313.882.8584

From: Silvia, Tovar-Rivera [mailto:S.TovarRivera1212@email.ncu.edu]

Sent: Wednesday, March 29, 2017 11:55 AM

To: akohnke@ltu.edu

Subject: Permission to adopt and modify survey questions from your study entitled: Incorporating UTAUT predictors for understanding home care patients' and clinician's acceptance of healthcare telemedicine equipment

Dr. Bush, Dr. Cole, and Dr. Kohnke:

I am currently pursuing a PhD in Business Administration with computer and information security specialty from Northcentral University, Prescott, Arizona. To fulfill the requirements of this degree, I am conducting a quantitative research focused on examining the ergonomics issues surrounding the United States (U.S.) public's intention to adopt a Combined Biometric and Smart Card Technology (CBIOSCT) as an alternative to current forms of identification for identity theft and identity fraud prevention. For my research, I need to compile a survey instrument that can be administered online. Therefore, I would like to request your permission to adopt and modify survey questions from your study entitled: Incorporating UTAUT predictors for understanding home care patients' and clinician's acceptance of healthcare telemedicine equipment.

I look forward to receiving your consent to use and modify the instrument for my dissertation.

I will be sure to provide adequate reference to your work in my dissertation.

Please contact me at: S.TovarRivera1212@email.ncu.edu

Thank you,

Sincerely,

Silvia Tovar-Rivera
Doctoral Candidate
Northcentral University, AZ
USA

Appendix I: Models and Theories of Individual Acceptance

Models and Theories	Constructs
Theory of reasoned action (TRA) by Fishbein and Ajzen (1975), derived from psychology to measure behavioral intention and performance.	Attitude Subjective norm
Technology acceptance model (TAM) by Davis (1989) included a new scale with two specific variables to determine user acceptance of technology.	Perceived usefulness Perceived ease of use
Technology acceptance model 2 (TAM2) by Venkatesh and Davis (2000) is adapted from TAM and includes more variables.	Subjective norm, ^a experience, ^a voluntariness, ^a image, ^a job relevance, ^a output quality, ^a and result demonstrability ^a
Motivational model (MM) also stemmed from psychology to explain behavior. Davis et al. (1992) applied this model to technology adoption and use.	Extrinsic motivation Intrinsic motivation
Theory of planned behavior (TPB) by Ajzen (1991) extended TRA by including one more variable to determine intention and behavior.	Attitude Subjective norm Perceived behavioral control
Combined TAM and TPB (C-TAM-TPB) by Taylor and Todd (1995).	Perceived usefulness, perceived ease of use, attitude, subjective norm, and perceived behavioral control
Model of PC utilization (MPCU) by Thompson et al. (1991) represented an adjustment from the theory of attitudes and behavior by Triandis (1980) to predict PC usage behavior.	Social factors, affect, perceived consequences (complexity, job-fit, long-term consequences of use), facilitating conditions, and habits
Innovation diffusion theory (IDT) by Rogers (1962) who adapted the theory to include the information systems innovations of Moore and Benbasat (1991), who identified five attributes from Rogers' model and two additional constructs.	Relative advantage, ^b compatibility, ^b complexity, ^b observability, ^b and trialability. ^b image and voluntariness of use
Social cognitive theory (SCT) by Bandura (1986) applies to information systems by Compeau and Higgins (1995) to determine usage.	Encouragement by others, others' use, support, self-efficacy, performance outcome expectations, personal outcome expectations, affect, and anxiety.
Unified theory of acceptance and use of technology model (UTAUT) by Venkatesh et al. (2003) integrated the above theories and models to measure user intention and usage on technology	Performance expectancy, effort expectancy, attitude toward using technology, social influence, facilitating conditions, self-efficacy, and anxiety.

Note. This table outlines the concept of the UTAUT system and the notions of the eight theories/models that Davis et al. (2003) studied to formulate this system. Adapted from Sundaravej (2009, pp. 3-4).

^a Indicates TAM2 only.

^b Indicates Roger's constructs.

Appendix J: Frequency Table for Survey Items in the Demographic Information Section*Current residence*

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid New York, NY	25	17.2	17.2	17.2
Washington, DC	32	22.1	22.1	39.3
Orlando, FL	32	22.1	22.1	61.4
Charleston, SC	3	2.1	2.1	63.4
Las Vegas, NV	31	21.4	21.4	84.8
San Francisco, CA	22	15.2	15.2	100.0
Total	145	100.0	100.0	

Legally eligible for a State Driver's License or Identification card

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Yes	145	100.0	100.0	100.0

Age group

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 18-24 years old	5	3.4	3.4	3.4
25-45 years old	26	17.9	17.9	21.4
46-63 years old	59	40.7	40.7	62.1
64 years old and above	55	37.9	37.9	100.0
Total	145	100.0	100.0	

Gender

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Male	41	28.3	28.3	28.3
Female	104	71.7	71.7	100.0
Total	145	100.0	100.0	

Highest level of education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High school degree or equivalent	27	18.6	18.6	18.6
	Bachelor of Science/Arts or equivalent	62	42.8	42.8	61.4
	Master's degree or equivalent	34	23.4	23.4	84.8
	Doctoral degree or equivalent	10	6.9	6.9	91.7
	Medical or Law degree or equivalent	6	4.1	4.1	95.9
	Other	6	4.1	4.1	100.0
	Total	145	100.0	100.0	

Annual household income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	\$50,000 or less	48	33.1	33.1	33.1
	\$50,001 - \$100,000	46	31.7	31.7	64.8
	\$100,001 - \$150,000	31	21.4	21.4	86.2
	\$200,001 or more	20	13.8	13.8	100.0
	Total	145	100.0	100.0	

Appendix K: Summary of Constructs and Corresponding Survey Items

Factor	Name	Questions under the factor
BI-DV	BI to use CBIOSCT	<ol style="list-style-type: none"> 1. I intend to use CBIOSCT for identification purposes (BI1). 2. I predict I would use CBIOSCT for identity theft and fraud prevention (BI2). 3. I plan to continue to use CBIOSCT in the future for identity theft and fraud prevention (BI3).
PE-IV	PE	<ol style="list-style-type: none"> 1. Using CBIOSCT will protect me against identity theft (PE1). 2. Using CBIOSCT will enhance the reliability of my personal data thus protect me against identity fraud (PE2). 3. Using CBIOSCT allows for an effective identity verification and authentication process (PE3).
PC-IV	PC	<ol style="list-style-type: none"> 1. CBIOSCT is difficult to be forged by criminals (PC1). 2. Using CBIOSCT is secure (PC2). 3. CBIOSCT limits unauthorized access to users' personal information (PC3).
SI-IV	SI	<ol style="list-style-type: none"> 1. People who are important to me influence my intention to use the CBIOSCT (SI1). 2. People I know who are using CBIOSCT at their workplace influence my intention to use CBIOSCT (SI2). 3. The United States government's encouragement influences my intention to use the CBIOSCT (SI3).
FC-IV	FC	<ol style="list-style-type: none"> 1. CBIOSCT infrastructure is available in government and private sectors for identity authentication and fraud risk detection (FC1). 2. A customer service contact center is available to answer CBIOSCT users' inquiries (FC2). 3. Current driver's licenses and state ID cards embedded technology are likely to be phased out soon (FC3).
ATT-IV	Att	<ol style="list-style-type: none"> 1. The use of a CBIOSCT in existing forms of personal identification in the U.S. to combat identity theft and identity fraud is a good idea (Att1). 2. I feel that the use of CBIOSCT for identity theft and identity fraud prevention is beneficial (Att2). 3. The use of CBIOSCT would enhance our standard of living (Att3).

Appendix M: Reproduced Correlations and Total Variance

Table M1.

Reproduced Correlations.

		Reproduced Correlations								
		PE1	PE2	PE3	PC1	PC2	PC3	SI1	SI2	SI3
Reproduced Correlation	PE1	.589 ^a	0.690	0.563	0.519	0.584	0.583	0.056	0.085	0.152
	PE2	0.690	.892 ^a	0.708	0.595	0.670	0.682	0.201	0.170	0.284
	PE3	0.563	0.708	.577 ^a	0.478	0.520	0.542	0.078	0.089	0.186
	PC1	0.519	0.595	0.478	.624 ^a	0.674	0.575	0.129	0.128	0.199
	PC2	0.584	0.670	0.520	0.674	.850 ^a	0.721	0.343	0.299	0.342
	PC3	0.583	0.682	0.542	0.575	0.721	.662 ^a	0.243	0.226	0.278
	SI1	0.056	0.201	0.078	0.129	0.343	0.243	.741 ^a	0.483	0.491
	SI2	0.085	0.170	0.089	0.128	0.299	0.226	0.483	.337 ^a	0.335
	SI3	0.152	0.284	0.186	0.199	0.342	0.278	0.491	0.335	.378 ^a
	FC1	0.486	0.560	0.445	0.370	0.540	0.545	0.244	0.214	0.238
	FC2	0.316	0.308	0.274	0.151	0.348	0.390	0.152	0.173	0.161
	FC3	0.303	0.388	0.319	0.143	0.261	0.322	0.149	0.139	0.172
	Att1	0.423	0.467	0.359	0.299	0.446	0.444	0.057	0.112	0.076
	Att2	0.567	0.620	0.478	0.390	0.589	0.596	0.113	0.160	0.119
	Att3	0.373	0.405	0.305	0.242	0.434	0.430	0.164	0.180	0.133
	BI1	0.380	0.451	0.369	0.240	0.428	0.442	0.108	0.176	0.167
	BI2	0.418	0.471	0.387	0.307	0.493	0.484	0.068	0.159	0.142
	BI3	0.339	0.423	0.359	0.184	0.369	0.405	0.126	0.186	0.200
Residual ^b	PE1		0.029	-0.041	-0.019	0.004	0.019	0.001	-0.021	0.003
	PE2	0.029		-0.007	-0.013	0.010	-0.011	-0.014	0.017	0.011
	PE3	-0.041	-0.007		0.048	-0.019	-0.010	0.008	-0.025	0.005
	PC1	-0.019	-0.013	0.048		0.008	-0.027	0.013	0.001	-0.017
	PC2	0.004	0.010	-0.019	0.008		0.022	0.002	0.013	-0.022
	PC3	0.019	-0.011	-0.010	-0.027	0.022		-0.017	0.001	0.028
	SI1	0.001	-0.014	0.008	0.013	0.002	-0.017		-0.008	0.016
	SI2	-0.021	0.017	-0.025	0.001	0.013	0.001	-0.008		-0.015
	SI3	0.003	0.011	0.005	-0.017	-0.022	0.028	0.016	-0.015	
	FC1	0.021	-0.017	0.028	0.016	-0.037	-0.003	-0.013	0.035	0.008
	FC2	-0.007	0.006	-0.016	0.003	0.005	-0.006	0.000	-0.021	0.018
	FC3	-0.020	0.009	0.017	-0.014	0.024	0.011	0.022	0.016	-0.061
	Att1	-0.029	0.006	0.018	-0.005	0.004	0.013	-0.025	0.048	-0.013
	Att2	0.014	-0.013	-0.003	0.001	-0.007	0.019	0.030	-0.052	0.012
	Att3	-0.013	0.006	0.014	-0.002	0.012	-0.032	-0.008	0.021	-0.015
	BI1	0.033	0.014	-0.045	-0.016	0.030	-0.022	0.008	-0.026	0.004
	BI2	-0.007	-0.001	0.004	0.025	-0.037	0.004	0.009	-0.011	0.008
	BI3	-0.005	-0.021	0.037	-0.002	-0.004	0.008	-0.016	0.028	0.005

Extraction Method: Principal Axis Factoring.

a. Reproduced communalities

b. Residuals are computed between observed and reproduced correlations. There are 2 (1.0%) nonredundant

Table M2.

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings ^a
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	7.73	42.97	42.97	7.45	41.39	41.39	6.07
2	1.93	10.71	53.68	1.60	8.88	50.27	5.07
3	1.63	9.04	62.71	1.24	6.89	57.16	5.69
4	1.13	6.30	69.01	0.75	4.18	61.34	2.61
5	0.81	4.50	73.52	0.48	2.64	63.98	4.04
6	0.69	3.86	77.37	0.31	1.71	65.69	0.75
7	0.60	3.32	80.69				
8	0.55	3.05	83.74				
9	0.50	2.79	86.53				
10	0.44	2.46	88.99				
11	0.38	2.12	91.10				
12	0.36	2.03	93.13				
13	0.34	1.87	95.00				
14	0.25	1.39	96.39				
15	0.21	1.16	97.55				
16	0.19	1.03	98.58				
17	0.14	0.76	99.34				
18	0.12	0.66	100.00				

Extraction Method: Principal Axis Factoring.

^a When factors are correlated, sums of squared loadings cannot be added to obtain a total

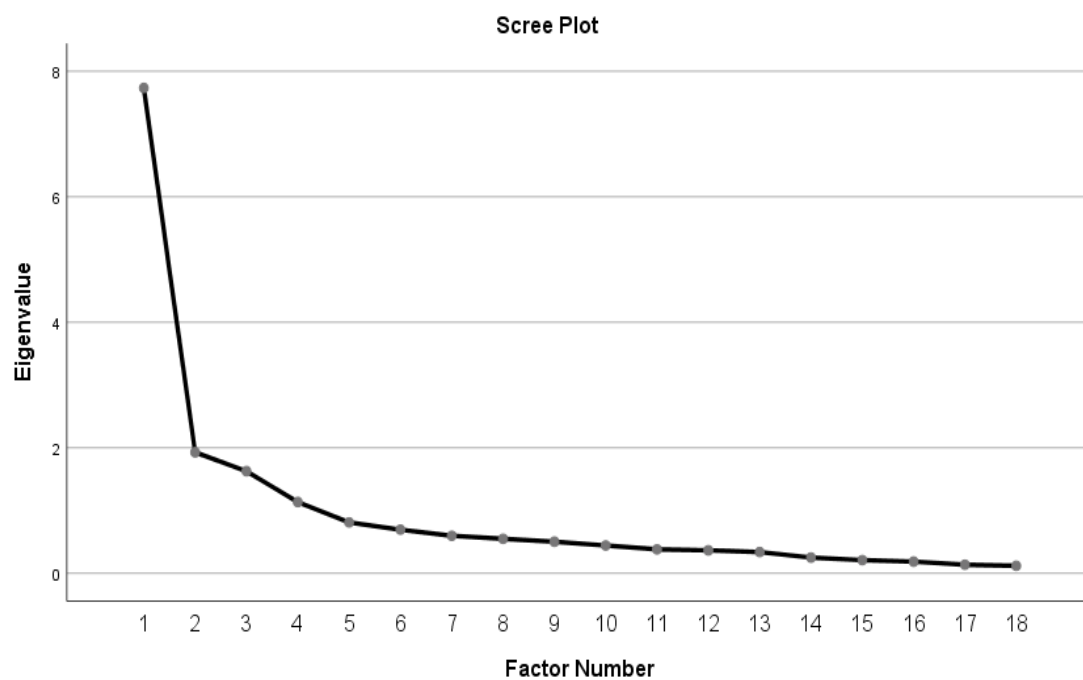
Appendix N: Scree Plot of Eigenvalues

Figure N1. Scree Plot of Eigenvalues.

Appendix O: Multicollinearity Diagnostics

Table O1.

Multicollinearity Diagnostics

Pearson Correlations (N = 145)							Collinearity Statistics Coefficients ^a	
	PE	PC	SI	FC	Att	BI	Tolerance	VIF
Performance Expectancy (PE)	1						0.369	2.709
Perceived Credibility (PC)	.750 ^b	1					0.382	2.619
Social Influence (SI)	.209 ^c	.347 ^b	1				.842	1.188
Facilitating Conditions (FC)	.544 ^b	.476 ^b	.286 ^b	1			0.621	1.611
Attitude (Att)	.573 ^b	.548 ^b	.172 ^c	.508 ^b	1		0.593	1.688
Behavioral Intention (BI)	.503 ^b	.460 ^b	.202 ^c	.493 ^b	.730 ^b	1		

^a Dependent Variable: Behavioral Intention.

^b Correlation is significant at the 0.01 level (2-tailed).

^c Correlation is significant at the 0.05 level (2-tailed).

Appendix P: SEM Parsimonious Model Multicollinearity Diagnostics

Table P1.

SEM Parsimonious Model Multicollinearity Diagnostics

		Coefficients^a					
		Unstandardized Coefficients		Standardized Coefficients		Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Tolerance VIF
SEM	(Constant)	0.158	0.196		0.807	0.421	
	PE	-0.165	0.101	-0.132	-1.636	0.104	0.298 3.354
	FC	0.328	0.115	0.203	2.842	0.005	0.381 2.624
	SI	0.121	0.060	0.102	2.016	0.046	0.758 1.319
	Att	0.819	0.083	0.773	9.863	0.000	0.316 3.165

^a Dependent Variable: BI.

Appendix Q: SEM Parsimonious Model Multicollinearity Diagnostics

	Att_IV	SI_IV	FC_IV	PE_IV	BI_DV
Att_IV	1				
SI_IV	0.167	1			
FC_IV	0.73	0.342	1		
PE_IV	-0.084	0.072	-0.103	1	
BI_DV	0.836	0.247	0.705	0.001	1