2007

A study of biometric authentication adoption in the credit union industry

Dawn Delaine Laux
Iowa State University

A study of biometric authentication adoption in the credit union industry

by

Dawn Delaine Laux

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Systems

Program of Study Committee:
Brian Mennecke, Major Professor
Michael Crum
Sree Nilakanta
Kevin Scheibe
Anthony Townsend

Iowa State University

Ames, Iowa

2007

UMI Number: 1443068

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

TABLE OF CONTENTS

ABSTRACT

Society has become more dependent on technology for identification purposes because the intimacy of a simple face to face acknowledgement of a person's identity has become a thing of the past. The purpose of this study is to understand the factors that influence the intent to adopt biometric authentication in organizations using the theory of adoption and diffusion of innovations. Using external pressure, readiness and perceived benefits, the research model measures the level of contribution that these factors make to the adoption of biometric authentication in the credit union financial services. Within the three main factors, the sub-factors that contribute to the model are competitive pressure, consumer pressure, regulatory pressure, innovativeness, top management support, consumer readiness, financial resources, and perceived benefits. Based on the sub-factors, the results indicate that the intent to adopt is driven by competitiveness and finances and not by the perceived benefits within the credit union industry.

CHAPTER 1. INTRODUCTION

Society has become more dependent on technology for identification purposes because the intimacy of a simple face to face acknowledgement of a person's identity has become a thing of the past. Transacting business with an organization such as a financial institution now requires a more sophisticated, technology based approach with the addition of electronic services outside of the traditional brick-and-mortar branch location. For instance, before the integration of direct deposit and ATMs, a teller may have seen the same customers weekly. Now a teller may rarely see the same customers in a month. Identifying a customer by face to face recognition would be irresponsible given the lack of frequency in visits to the branch. Even the act of displaying an identification card at the teller line may not be sufficient. So how does an organization verify an individual's identity? There are three basic approaches for verification: 1) by using something you have (an ATM card), by using something you know (a password or PIN) or by using something unique about yourself that cannot be shared (Bolle, Connell, Pankanti, Ratha, and Senior, 2004; Miller 1994). Since there are an increasing number of channels to transact financial information, the amount of security to protect these channels is increasing as well. With the increase in the electronic channels offered through retail organizations and financial institutions, there is greater access through the Internet to individual information that was once considered private. The result is an augmentation of identity theft and account hijacking.

According to a 2005 report by the FTC (2006) on identity theft complaints, there were over 700,000 complaints in the last 3 years. In addition, a 2006 Identity Fraud Survey Report was released by the Council of Better Business Bureaus and Javelin Strategy &

Research stating that 8.9 million people were the victims of identity fraud in the United States in the last year, and that the total one-year cost of identity fraud in the United States is at $56.6 billion (Better Business Bureau, 2006). The FDIC published a report in 2004 on account hijacking and identity theft and how organizations must improve security measures to control the amount of fraud occurring each day. The difference between identity theft and account hijacking is that identity theft occurs when an unauthorized individual uses another person's personal information to commit fraud. The act of account hijacking is when an individual gains unauthorized access to another person's account by way of phishing or hacking (FDIC, 2004). In order to combat these security issues, new legislation has been passed as well as new technological advances. One potential option for increased security that has been recently receiving a considerable amount of attention is biometric authentication.

While biometric usage has been around for a number of years, recent events have propelled its popularity as a viable option for additional security measures. Biometrics is a term used to describe the use of physiological or behavioral characteristics to verify an individual's identity (Bolle et al., 2004). Physiological biometrics is a physical measurement such as the verification of a fingerprint, hand, eye or face. Behavioral biometrics takes a measurement of how an action takes place, such as a signature. These characteristics can be measured by the following requirements as a qualifying biometric: universality, distinctiveness, permanence and collectability (Zorkadis and Donos, 2004; Prabhakar, Pankanti, and Jain, 2003; Jain, 2004). With biometrics, there are two types of authentication methods that can be used: identification and verification (Bolle et al., 2004). Both methods begin in the same fashion. During an enrollment process, a template is created and stored in

a database. If the method chosen is identification, it is a one-to-many search in the database. For example, an authentication of an individual's hand print alone would be compared to an entire database of hand print records to find a match. The alternative method is verification. Each individual's biometric record is coupled with a unique identifier. The system first searches the database for the identifier (an account number, for example) and then verifies that the biometric from the input device matches the individual's stored biometric assigned to that particular identifier. It is a one-to-one or one-to-few search for the biometric portion of the authentication process. In either method, the individual is authenticated with something that is owned. Using this type of authentication would increase the level of security on an individual's account because the system can validate that the actual account holder is the one requesting access. When an individual uses a password, it can be compromised by others or even forgotten by the account holder.

With the recent advancements and concern for increased security, biometric authentication has yet to be implemented in large scale proportions. While the adoption of this new technology is limited, it is steadily increasing. There are various industries that are interested in the adoption factors of this type of technology such as healthcare, government agencies, retail, and financial institutions. These successful and innovative organizations are concerned about providing the best security possible while still upholding customer service expectations of the consumer. The technology can not be successful if the consumer will not accept it; it needs to be easy to use, convenient and give the consumer the feeling of control (Coventry, De Angeli, and Johnson, 2003).

There is significant research on the theory of adoption and diffusion of innovations. Whether the research involves individual decision making or organizational decision making,

the innovation-decision process involves a progression in which an individual or an organization evaluates a new plan and decides whether or not it is worth incorporating into practice (Rogers, 2003). The decision stage of the innovation-decision process is the point at which an organization adopts or rejects an innovation. In order for an organization to make profitable innovation decisions, understanding the factors that influence the implementation process is significant (Frambach and Schillewaert, 2002). The focus of this study concentrates on the factors that influence the adoption of biometric authentication technology on an organizational level.

1.1 Research Problem

Research examining the adoption of biometric technologies is limited due to the low levels of biometric system adoption. Conversely, the interest level is escalating with the increase of identity theft, so now is an opportune time to study the factors that influence this new technology. In the case of this study, the focus of the research model is on the credit union industry. The primary research question is, would a credit union adopt biometric authentication because of external pressures such as consumer, regulatory, and competitive pressures? Also, does the level of readiness influence the intent to adopt? Finally, would the perceived benefits of biometric authentication influence the intent to adopt?

The amount of research on biometric authentication adoption by organizations is limited primarily because of the infancy of biometric authentication implementations. Many of the research studies that are available discuss the attributes of biometric authentication and discuss reasons that organizations have been slow to adopt this technology (Jain et al, 2004; Harris and Yen, 2002; Fairhurst, 2003). NCR Financial Solutions Division performed a

study on the use and viability of iris verification at automated teller machines (ATM) (Coventry et al, 2003). In a study by Moody (2004), a survey was conducted in order to understand the perceptions of individuals on the acceptance of biometric authentication. While each of these studies includes valuable information about the adoption of biometric authentication methods, they have not surveyed organizations about their opinions of the factors that influence the decision to adopt. By reaching out to other domains for guidance, there have been research studies that have addressed this issue for other innovative technologies such as EDI, E-Commerce, and mobile banking. By utilizing this prior research, the current study on biometric authentication will add to the biometric research domain in a way that has been not been done before.

The purpose of this study is to understand the factors that influence the intent to adopt biometric authentication in organizations by way of the methods found in the theory of adoption and diffusion of innovations. In an examination of prior research, the model used for this particular biometric authentication study is adapted from an EDI adoption model (Chwelos, Benbasat, and Dexter, 2001; Iacovou, Benbasat and Dexter, 1995), as well as additional factors from adoption research by Srinivasan, Lilien, and Rangaswamy (2002) and Tsikriktsis, Lanzolla, and Frohlich (2004). The intention of this paper is to use the EDI (electronic data integration) adoption model that was originally purposed by Iacovou, Benbasat and Dexter (1995) and utilize the factors of perceived benefits, external pressure and readiness into a study of organizational biometric technology adoption. This paper begins with a review of biometric technology, examples of how it is currently being used in financial institutions, and prior research of biometric studies as well as a review of adoption research and prior studies of the adoption of other innovative technologies. Following this,

the theoretical framework is discussed along with the research methods and procedures. The paper ends with the results, a discussion of the results, and the paper's conclusion.

CHAPTER 2. REVIEW OF LITERATURE

The purpose of this study is to research the theory of technology adoption that relates external pressures, readiness and perceived benefits with the intention to adopt biometric authentication. A better understanding of the factors that influence organizations to adopt a new technology such as biometric authentication would assist in improving the rate of adoption for this technology. The two foundations of research for this literature review are biometric technology research and the adoption of innovations research.

The biometric technology section provides an overview of the definition of biometric technology, the different types of biometric authentication methods, and biometrics' value as a security tool. As with any new technology, it is important to review the current criticisms and concerns that are published as well as ethical issues facing biometric authentication. Although prior research on biometrics is limited, it is a valuable resource when developing the tools necessary for the research performed in this study.

The next section of the literature review focuses on prior adoption research. Two streams of research on adoption are prevalent in the literature: research involving individual and organizational technology adoption. The focus of this study is on the latter, organizational adoption. A review of the perceived attributes of innovation and the innovation decision process described by Rogers will then follow, as well as examples of organizational adoption research in related areas such as EDI, E-Commerce, and mobile banking. The adoption literature in these domains follow a similar research model as the one proposed for the current study. This review concludes with a few examples of how biometric authentication is currently being used in financial institutions.

2.1 Biometrics Technology

Biometrics is a method of identifying individuals that has been in operation for several years. Each of us routinely uses biometric identifiers such as voice and facial characteristics to recognize family and friends. Recent prominent security lapses have brought an increase in awareness of the need for greater security measures, so biometrics have been transformed into an authentication technology that can be automated. There is an increase in the level of security for an individual's account because biometric systems reliably validate that the enrolled account holder is the one requesting authorization. This is the main difference between the use of biometrics and passwords because passwords can be compromised, shared, or forgotten. A basic definition of biometrics involves the use of physiological or behavioral characteristics to verify an individual's identity (Bolle et al., 2004). Physiological biometrics is a physical measurement such as the verification of a fingerprint, hand, eye or face. Behavioral biometrics takes a measurement of how an action takes place, such as a signature. In order for a measurement to qualify as biometric, certain requirements must be met (Zorkadis and Donos, 2004; Prabhakar et al, 2003; Jain, 2004):

- *Universality*. Each person should have the biometric characteristic.
- *Distinctiveness*. The characteristic must be distinct among persons and no two should be alike.
- *Permanence.* The characteristic must remain invariant over a period of time.
- *Collectability*. The characteristic can be measured quantitatively and easy to collect.

- *Performance*. In terms of a biometric system, the performance should be practical in its accuracy, speed and resource requirements.
- *Acceptability*. It is the extent to which intended users will accept the system.
- *Circumvention*. Refers to how the well the system can detect attacks that are fraudulent.

With all biometric measurements and corresponding requirements, there are two methods of authentication.

2.1.1 Biometric Authentication

Authentication is described as the process of determining the identity of a communicating party (Bolle et al., 2004). As stated before, there are two types of biometric authentication methods that can be used: identification and verification. If the method chosen is identification, it is a one-to-many search in a database of participants' biometric records. It would be the sole means of identification for an individual requesting access. The alternative method is verification. It is considered a one-to-one or one-to-few search in the authentication process. Each individual's biometric record is stored in a database along with an additional unique identifier such as an account number. When an individual attempts to perform a transaction on a biometric system that uses the verification system, it first performs a search on the database for the submitted identifier and then verifies that the biometric scan from the sensor matches the individual's stored biometric record assigned to that particular identifier. In either method, individuals are authenticated with something that is unique to them that cannot be shared, borrowed or lost. Once an authentication method is chosen by an organization, the next step is the enrollment process.

2.1.2 Enrollment Process

In the development of the enrollment process, it must first follow a determined enrollment policy due to the fact that very private information will be supplied to the organization that will in turn be required to protect it (Bolle et al., 2004). As stated before, the concept of biometric authentication is that the system verifies the identity of the individual requesting access by confirming a unique physical or behavior characteristic that matches a similar stored record in a database. This is why it is imperative that the true identity of the individual enrolling is in fact correct. The biometric verification method is not capable of determining the true identity of an individual. The enrollment policy has the responsibility of verifying a person's identity even before the technology portion of enrollment begins.

Once an individual is verified, the physical enrollment can proceed. Depending on which type of biometric is used, a template or model is created from the unique characteristics of an individual for that particular biometric reader. In order to create the template, the reader, or sensor, takes specific samples of data from the subject and converts the data into a mathematical record to be stored in a database. In the case of a verification method, this mathematical record would be coupled with a unique number (for instance, an account number). A template can contain multiple records for the same individual for an improved acceptance rate when the opportunity comes to apply it beyond the initial enrollment period. Once the enrollment process is complete, the subsequent attempts for access behind a biometric authentication system will compare the individual's live scan to the stored template in the database (FDIC, 2004; Bolle et al., 2004). The behavioral biometric method uses the same general process except that it uses models instead of

mathematical templates. One of the drawbacks in the biometric enrollment process is that it is not 100% accurate.

2.1.3 Error Rates

There are two classes of errors in the accuracy of biometric authentication. The first issue is called a False Acceptance Rate, or FAR. The FDIC report describes a False Acceptance Rate as "the probability that the system will accept a false biometric credential as legitimate" (FDIC, 2004; p. 30). FAR occurs when, for example, an individual requesting access to his or her account, instead is given access to another person's account. The other issue is called a False Reject Rate, or FRR. The FDIC report describes a False Reject Rate as "the probability that the system will reject a valid biometric credential" (FDIC, 2004; p. 30). This would be an issue when a legitimate individual is denied access because the biometric authentication system cannot match the person's live scan with any records in the database. These issues are the reason why current biometric authentication systems are primarily an additional level of security versus a sole method of authentication. There are many biometric identifiers currently under development, but the more common biometrics technologies in use and in production is described in the following section.

2.1.4 Types of Biometrics

There are various biometrics in research which can vary with anything from a person's fingerprint to the way that he or she walks, but for the purposes of this study the most common biometrics will be described. These include fingerprint, facial recognition, hand geometry, iris, and voice recognition. The International Biometric Group performed a

research study on the use of biometrics in the market, and the following table displays how each of these biometrics break out by market share in 2006 (see Table 1).

Table 1. *Percent of Biometric Market by Technology in 2006*

Biometric	Percentage of Market
Fingerprint	44%
Face	19%
Hand Geometry	9%
Iris	7%
Voice	4%

Source: Biometrics Market and Industry Report 2006-2010 (International Biometric Group, 2006)

2.1.4.1 Fingerprint Recognition

Fingerprint recognition is the most widely used method of biometric authentication. The technology uses unique features from the fingerprint to develop the template. These features are known as minutiae, which are a combination of ridge bifurcations and ridge endings. The template only uses the information gathered describing the minutiae of the fingerprint and not the entire image of the fingerprint. This is important to note because it is not possible to reconstruct an image of the fingerprint from the information stored in the database. There are advantages and disadvantages to a fingerprint biometric authentication system.

One advantage of fingerprint recognition is that it has a long history of use. In relative terms, the use of fingerprints as an automated authentication tool is new compared to the centuries of manual fingerprinting of individuals for identification. Other advantages

include factors such as the ability to use multiple fingers to scan for a template, the fingerprint is permanent and it does not change patterns with age, it is easy to use, and the sensors are inexpensive (NSTC, 2005). The disadvantages of fingerprint recognition include issues with public perceptions about its use such as touching the sensor will spread germs and the scanned image of the fingerprint could be reproduced or used for criminal investigations (NSTC, 2005). Research has also been performed on print quality in elderly individuals, which shows that as people grow older, there is a higher rate of reject rates in sensor recognition (Theofanos, Micheals, Scholtz, Morse, and May, 2006).

2.1.4.2 Face Recognition

As stated before, humans have been using facial recognition to identify one another as a part of daily life for centuries. There are two categories of facial recognition: facial appearance and facial geometry (Bolle et al., 2004). The method of facial appearance is also called the eigenface method because it collects a number of face images that form a two-dimensional gray-scale image which in turn produces a biometric template (FDIC, 2004). Facial geometry gathers measurements of the face that do not change over time such as the distance between the eyes and the length and width of the face.

In contrast to fingerprint biometrics, there is no contact made in facial recognition biometrics. The disadvantage to this type of biometric is that the condition of the environment while obtaining the sample can affect the quality of the image (FDIC, 2004). Poor lighting, camera quality, and obstructions on the face by the individual requesting access can make a significant difference in the initial enrollment as well as subsequent attempts for access (NSTC, 2006).

2.1.4.3 Iris Recognition

Iris recognition uses the pattern of the iris as a unique identifier. Although the coloration of the iris is found to be genetic, the pattern of the iris results from the development process of the eye during the prenatal stage of growth (Bolle et al., 2004; NSTC 2006). A high resolution digital camera is used as the sensor for acquiring the image of the iris. An individual must line his or her eye up within a field of view in order to minimize the amount of noise (i.e., eyelashes, eyelids) in the image.

Just as with the facial recognition biometric, there is no physical contact with a sensor. Noise such as eyelids, eyelashes, and contact lenses can decrease the accuracy of the biometric. There is also a negative public misperception that the eye is scanned with a light source, and that it would damage the eye (NSTC, 2006). Although the automated technology is new and consumer education is needed to reduce fears, research has found it to be very accurate (Bolle et al., 2004).

2.1.4.4 Hand Geometry

Hand geometry analyzes the geometrical structure of the human hand. An individual places his or her hand onto a guided plate where the system measures the length, width, thickness, and surface area (NSTC, 2006). The enrollment template is created when two to three silhouette images are captured, measured, and then averaged. It is a less intrusive process than the iris recognition method, but also a less accurate one because the geometrical shape of the hand is less unique. The technology has a high false acceptance and false rejection rate (Bolle et al., 2004). Consequently, this technology is not suitable as an identification method, but rather as a verification method with an additional level of security.

2.1.4.5 Voice Recognition

Voice recognition, also called Speaker recognition, uses an individual's voice characteristic for recognition purposes (NSTC, 2006). It is important to note that this technology should not be confused with "speech recognition" which recognizes the words that are spoken, regardless of who speaks them. The approach to developing a template for an individual's voice print is accomplished by recording speech samples over multiple attempts in order to increase the accuracy rate.

One advantage to voice recognition is that the sensor needed to acquire the voice print is commonly available (i.e., telephones, cellphones) (NSTC, 2005). One of the disadvantages that have caused the need for more sophisticated technology is the threat of replay attacks where an unauthorized person attempts to gain access with a recorded version of the authorized user's voice. Another disadvantage is that there can be a high false accept rate if a person has a cold or there is noise on the sensor (Bolle et al., 2004).

2.1.5 Prior Research

In a review of the research available concerning biometric technology, various types of research has emerged. There are studies available that are definitional in nature, such as an article by Sanderson and Erbetta (2000) which primarily outlines biometric technology as well as the different types of biometrics available. The researchers concluded from this information that the most suitable biometric technology for military battlefield requirements would be iris scanning due to the environmental conditions found on the battlefield. In an article by Whisenant (2003), the researcher bases a review of various biometrics as the reasoning behind his proposition that facial recognition integrated with an additional

biometric, such as fingerprint recognition, would be a non-intrusive solution for sport venue management in deterring terrorist attacks.

2.1.5.1 Security Controls

Another focus of research in biometrics involves the benefits of biometric technology as a method of security control. For example, Harris and Yen (2002) study the benefits of biometric technology over the use of person identification numbers (PINs), cards or tokens for access to secure systems. They point out that with PINs, cards, and tokens an individual is identified as having the ability to access the information, whereas biometrics identifies the actual person requesting the access to the information. The purpose of their study is to provide information to organizations on the added security benefits of biometric technology and the need for stronger information assurance. This was accomplished by analyzing a set of pros and cons for biometric technology as well as six factors that would affect the adoption of biometrics. The six factors include economical, managerial, operational, technological, process-related, governmental and standards-related factors. In the analysis of this study, Harris and Yen find that biometric technology offers a level of security that cannot compare to traditional passwords. The researchers explain that biometrics offer multiple levels of security thresholds for how specific the individual's access request is to the template of the biometric stored in the database, and any concerns with biometric security can be remedied with proper education and awareness. While Harris and Yen discuss the need to use biometric technology as a greater level of security, an article by Ahmed and Siyal (2005) develop a system for enhancing the security of private keys with biometric technology. The researchers acknowledge the need for greater security in private keys due to the increase in

electronic commerce and the information that is being stored on smart cards. By analyzing the current method for assembling a private key, the researchers added another factor by including a biometric fingerprint. The result is an enhanced security mechanism for dynamically regenerating private keys with the use of an individual's fingerprint, password and smart card. As research is performed on the security benefits of biometric technology, there is equivalent research on the privacy concerns that surround it.

2.1.5.2 Privacy Concerns

Zorkadis and Donos (2004) produced an article analyzing the rising legal concerns related to the personal nature of biometric data as described in a paper by Prabhakar et al. (2003) where the researchers address three specific concerns: unintended functional scope, unintended application scope and covert recognition. For Zorkadis and Donos (2004), the purpose of the study is to explain the principles that must be followed by biometric systems to be in compliance with current legislation, and to propose a method for securing the privacy of an individual's information stored in a biometric database. This was accomplished by comparing the principles of purpose and the proportionality of biometric systems with current legal obligations. The researchers concluded that in order for biometric data to be kept private and follow current legislation rules, the following must occur: 1) the biometric identification data must only be used for the purpose that it was originally collected, 2) the data would be less accessible to others for further processing if it were to be stored in a device owned by the data subject (such as a smart card), and 3) the data controllers must be educated on the rights of data subjects and to be aware of the techniques available that prevent a re-identification issue.

In a related article pertaining to the issue of privacy, Alterman (2003), Langenderfer, and Linnhoff (2005) discuss the use of biometric identification systems in relation to ethical concerns for one's privacy. As with Prabhakar et al. (2003) and Zorkadis and Donos (2004), Alterman (2003) reiterates that the ensuing widespread deployment of biometric implementations must also provide a means for protecting the data from misuse. Ratha, Connell, and Bolle (2001) add to this concern with an article describing vulnerabilities in a biometric system and how to potentially prevent them with techniques that, if implemented, would decrease the threat of information theft.

2.1.5.3 Implementation Considerations

With security and privacy concerns in mind, the following research papers describe what it would entail to successfully implement a biometric system into an organization. Jain et al. (2004) identify in a discussion of pattern recognition the fundamental problems facing organizations when implementing biometric technology for widespread use: accuracy, scale, security and privacy. They further explain in detail how each of barrier requires further research and how each one stands in the way of widespread deployment. The researchers conclude that while there are adequate biometric systems deployed today on a small scale, not enough research has been performed on the wide use of sensitive personal data. As research projects are under way to answer the call of Jain et al., one paper in particular by Elliott, Kukula, and Sickler (2004) describes research projects being performed at Purdue University in biometric technology. The result has been that when implementing a biometric system into an organization, the researchers have identified a few important factors to consider: the environment that the biometric scanner will be placed in, the quality of the

image that is obtained, and the selection of the device used in acquiring the biometric element from an individual. In a related article, Sticha and Ford (1999) explain how the use of biometric technology has the potential in this industry to thwart duplicate enrollments and fraud found in the Food Stamp Program. Sticha and Ford (1999) found in their research that the biometric technology used must be acceptable to the user, accurate, resistant to fraud, and quick. Policy decisions are also vital to deterring fraud because fraud attempts occur most frequently at the point of enrollment.

In determining what barriers are in the way of implementation, Riley Jr. and Kleist (2005) studied the challenge organizations face when deciding if the implementation of a biometric system would be beneficial. The researchers identify a strategy for the decision making process by providing the reader with a step by step method in developing a business case specifically for the implementation of a biometric technology system. In addition to the previous paper, Kleist, Riley Jr., and Pearson (2005) produced a paper on a method for identifying how biometric technology may be a valuable tool in mitigating organizational risk based on the level of risk and type of biometric used. Chandra and Calderon (2005) provide a similar article for those organizations considering the implementation of a biometric authentication system by describing challenges, constraints and limitations of biometric technology that every organization should review while evaluating this type of technology.

2.1.5.4 Deployment Studies

While the use of automated biometric technology is new, some limited research has been performed on organizations with actual deployments. In a case study of a deployed

biometric system, Heracleous and Wirtz (2006) studied the role of biometric technology and how it might drive service excellence, productivity and security in the service industry. The researchers performed 16 interviews with top personnel at Singapore Airlines and the Civil Aviation Authority of Singapore pertaining to the use of biometrics in Singapore airports. The main implication drawn from this study is that an organization should not implement a new technology just for the sake of doing it; instead, organizations must be capable of strategic alignment and strategic innovation. Specifically, Heracleous and Wirtz (2006) found that not only is biometric technology a security improvement, but it must also unite with the organization's strategic initiatives towards service excellence to be successful. In a related article, Coventry et al. (2003) perform a study on customer driven usability as related to iris scanning authentication at ATMs (Automated Teller Machines). This research involved focus group studies to best understand consumer attitudes toward biometric technology, as well as the feasibility of how well iris scanning technology would perform with everyday ATM use. This involved a prototype and field test, and the researchers found that the input of consumers as well as exposure to prototype testing of this biometric technology system provided insight on how to improve user acceptance of this technology.

There are lessons to be learned in the prior studies of biometric deployment, such as the paper on the use of biometric technology in South Africa (Breckenridge, 2005). Breckenridge (2005) discusses how the United States is planning for a national system of biometric identification security, and that South Africa is already using biometrics; in particular, South Africa is utilizing this technology to improve the welfare system among other potential advancements. A point that Breckenridge (2005) makes is that the biometric deployment of South Africa has not gone well, and that there are lessons there to be learned

before the United States embarks on the same implementation plan of deploying widespread biometric systems.

2.2 Adoption Research

The amount of research performed on the adoption acceptance of new technologies among organizations and individuals is abundant. A significant goal of an organization is to best understand the factors that will increase the adoption of its new technology among users as well as determining which new technology is worthy of deployment in the first place. There have been many studies and many opinions on how to best analyze this issue, and researchers are looking for an exact explanation for that tipping point when a technology is accepted and deployed by a user or an organization. Is there a difference between how organizations accept a new technology and how a user accepts a new technology? Research has been done to attempt to clarify this situation by comparing prior research in both areas (Jeyaraj, Rottman, and Lacity, 2006). The study performed by these researchers includes a thorough breakdown of independent variables that are best and worst predictors of IT adoption research. Another focus of adoption research concentrates on the analysis of multiple models and deciding which performs the best, while others seek to combine constructs from multiple models to develop a new theory. The purpose of the study by Taylor and Todd (1995) was to compare three models of IT usage in order to determine the extent in which each can be used when attempting to understand the determinants of usage.

While Taylor and Todd (1995) reviewed three models, Venkatesh, Morris, Davis, and Davis (2003) analyzed eight models that utilize usage as a dependent variable and developed a unified model that incorporates the most significant constructs of those eight models. Once

the models where analyzed and users where surveyed with each of the eight models, they developed the Unified Theory of Acceptance and Use of Technology based on the constructs that were most significant. The resulting conclusion was that the significance level increased even more in a unified structure as opposed to eight separate models.

While Venkatesh et al. (2003) reviewed the theory of reasoned action, the technology acceptance model, the motivational model, the theory of planned behavior, a model combining the technology acceptance model and the theory of planned behavior, the model of PC utilization, the innovation diffusion theory, and the social cognitive theory, the review in this paper will focus on the innovation diffusion theory (Rogers, 2003) and how it can be utilized to study organizational adoption of biometric authentication technology. This is due to the fact that most EDI research studies are built on Roger's innovation diffusion theory (Iacovou et al., 1995), and Roger's theory is one of the few that has been used in organizational adoption studies (Jeyaraj et al., 2006).

2.2.1 Innovation Diffusion Theory

The diffusion of innovation theory developed by Rogers is characterized by five factors: innovation, individual, task, environmental and organizational. Within these factors, there are a multitude of characteristics that have been researched while all are seeking to explain the likelihood of adoption of an innovation (Mustonen-Ollila and Lyytinen, 2003; Moore and Benbasat, 1991). The five most generalized characteristics originally identified by Rogers were Relative Advantage, Compatibility, Complexity, Observability, and Trialability. Prior research in the Innovation Diffusion Theory has concentrated on one or more of these factors (Leonard-Barton and Deschamps, 1988; Moore and Benbasat, 1991;

Premkumar, Ramamurthy and Nilakanta, 1994; Subramanian and Nilakanta, 1996; Gopalakrishnan and Damanpour, 1997; Agarwal and Prasad, 1998; Ramamurthy, Premkumar and Crum, 1999; Suoranta and Mattila, 2004).

Whether the research involves individual decision making or organizational decision making, the innovation-decision process involves "a series of choices and actions over time through which an individual or a system evaluates a new idea and decides whether or not to incorporate the innovation into an ongoing practice" (Rogers, 2003). The decision stage of the innovation-decision process is the point at which an organization adopts or rejects an innovation, and consequently there are many views of how innovation impacts a firm's productivity, survival, growth and performance (Gopalakrishnan and Damanpour, 1997). Moore and Benbasat (1991) purposed a paper to describe the development of an instrument that is designed to measure an individual's perceptions of adopting a new technology innovation. They also state that it is generalized enough that it can be used to investigate how perceptions affect an individual's actual use of technology and innovations.

2.2.2 Prior Organizational Research

IT innovation adoption research has a rich body of research to pull from for information. In the detailed review by Jeyaraj et al. (2006), the researchers studied 51 prior organizational IT adoption publications from 1992 to 2003. They found that among the most frequently used independent variables, the best predictors of IT adoption by organizations were Top Management Support, External Pressure and Organization Size. The researchers suggest that adopter characteristics should also be researched as part of organizational adoption studies. This is also suggested in an article pertaining to future research by

Frambach and Schillewaert (2002). They state that beyond individual versus organizational factors, any factor used in determining whether or not to adopt and deploy a new innovation starts with understanding potential customers and what influences their adoption decisions. This includes the concept of organizational innovativeness (Srinivasan, Lilien, and Rangaswamy, 2002; Deshpande, Farley, and Webster, Jr., 1993). Deshpande et al. (1993) found that organizational innovativeness was related positively to organizational performance. The following organizational adoption studies have utilized at least one of these variables, and they are just an example of the body of knowledge that is available.

Grandon and Pearson (2004) examined factors that influence electronic commerce adoption in small and medium sized organizations. They focused on the perceptions of top management regarding the strategic value of electronic commerce. The factors used were organizational readiness, external pressure, and those of the Technology Acceptance Model (Davis, 1989). The researchers also looked to the research performed in electronic data interchange (EDI) to assist in forming their model, as there was limited research at the time in electronic commerce in small organizations. It was found from their results that the factors of external pressure, perceived ease of use (TAM) and perceived usefulness (TAM) were significant when influencing adoption, but organizational readiness was not.

In an empirical study of the different factors that contribute to the adoption of e-Processes by service firms, Tsikriktsis, Lanzolla, and Frohlich (2004) also incorporated external pressure into their research model. In this case, they described the concept of external pressure as the “bandwagon” effect. The other factors in their research model to predict the adoption of e-process were anticipated benefits, access to markets, internal barriers and customer barriers. Of the two electronic processes studied (e-CRM and e-

transactions), the one factor that was not significant in both was customer barriers. The researchers concluded that the forces driving the implementations outweigh the barriers preventing adoption of the processes by organizations.

Srinivasan, Lilien and Rangaswamy (2002) studied the adoption of radical technology by organizations. This included factors such as technological opportunism, institutional pressures (stakeholder and competitive), complementary assets, perceived usefulness, organizational innovativeness, and top management's advocacy. The factor of top management advocacy was defined by the researchers as "the efforts of the top management team to emphasize the importance of organizational responsiveness to new technologies." This was found to be a significant factor in the development of researcher's new construct of technological opportunism. In a related study by Ramamurthy, Premkumar, and Crum (1999), concluded that management support is necessary in confronting competitive pressures and facilitating the proper financial resources when faced with adopting a new innovative technology.

In relation to top management support, another perspective of influence is research pertaining to managerial influence and the interaction between perceived managerial behavior and employee characteristics when promoting the use of an innovation to the consumer (Leonard-Barton and Deschamps, 1988). This study found that while there was no direct relationship between management urging the use of an innovation and the subsequent increase of usage, the researchers did find that by analyzing the mediation of personal characteristics and skills with managerial intervention significant results were produced. Thus if an employee is already an innovative personality, the management influence was

small. If an employee was apprehensive in using a new innovation, management encouragement was important.

While these studies are just a few of the many studies on organizational adoption, they represent a basis to the study of biometric authentication adoption. The following biometric adoption studies have used different research models, but they all have a common goal: biometric adoption. The two researched biometric adoption studies focus on the individual adoption process, while the focus of this paper is on the organizational level.

2.3 Biometric Adoption Studies

In relation to biometric adoption research, two studies have focused on the acceptance of the technology by the individual. James, Boswell, Reithel, and Barkhi (2006) used the Technology Acceptance Model (TAM) to determine the intention to use security technologies, and in the case of this study, specifically the use of biometric technology devices. The researchers surveyed the faculty staff and students at the University of Mississippi to which they were able to acquire 298 usable responses for the analysis of the following constructs: perceived physical invasiveness, perceived usefulness, perceived ease of use and intention to use. James et al. (2006) state that the results of the study found that the perceived need for security and perceived ease of use positively impacted the individual's perception of the usefulness of the biometric device, yet perceived physical invasiveness of the device had a negative impact for adoption intention. In a similar study, Moody (2004) researches why biometrics adoption has been slow, and in turn attempts to identify the public perceptions of biometric technology. A survey instrument was developed and produced a

sample of 300 usable responses. Moody found that individuals responding to her survey are not ready to participate in the commercial use of biometric devices.

2.4 Biometric Technology in Financial Institutions

While there is not widespread use of biometrics in financial institutions, there are a few organizations utilizing the technology. NCR and Diebold have each deployed biometric enabled ATMs overseas according to an article in the ABA Banking Journal (Orr, 2006). Various financial institutions have found biometrics useful for safety deposit box access, self service kiosks and teller line transaction access (Giesen, 2006). The research in biometric technology has uncovered some common concerns among society. If an organization can be assured that these concerns have been identified and resolved, is this enough of a tipping point for acceptance of the technology? If that still does not invoke acceptance, is there a particular issue that cannot be overcome?

CHAPTER 3. FRAMEWORK

Based on the review of literature in biometric technology research and adoption research, a relation develops in how organizations can increase adoption of this technology in the retail industry. Biometric usage is in its infancy and organizations may not be educated enough on the concept of how it performs since very few of the population has been exposed to biometric technology. On the other hand, organizations are finding that this type of authentication method could prove to reduce costs and reduce fraud. The widespread use of biometrics is not yet here, but it is coming and there is a desire to understand how to win over the general population into adopting it.

By adapting the EDI adoption model used by Chwelos et al. (2001) and Iacovou et al. (1995), the following research objectives are the basis of this adoption framework:

1) Will organizations adopt biometric authentication because they perceive there is pressure to do so?
2) Does the level of perceived readiness affect how willing an organization is to adopt biometric authentication?
3) Would the perceived benefits of biometric authentication affect the organization's intention to adopt the technology?

The following research model attempts to answer the research objectives of this study. The goal of this study is to better understand the factors that are significant to organizations when making a decision as to whether not to adopt biometric technology as a means of added security for their member base.

3.1 Research Model

A model for biometric authentication was adapted from a previous study in EDI by Chwelos et al. (2001) which was adapted from the study by Iacovou et al. (1995). Using the three factors of external pressure, readiness and perceived benefits, the model measures the level of contribution that these factors make to the adoption of biometric authentication in the credit union financial services. The model found in Figure 1 presents each sub-factor and how each one contributes to its corresponding main factor. This in turn utilizes the main factors to explain the intention to adopt.

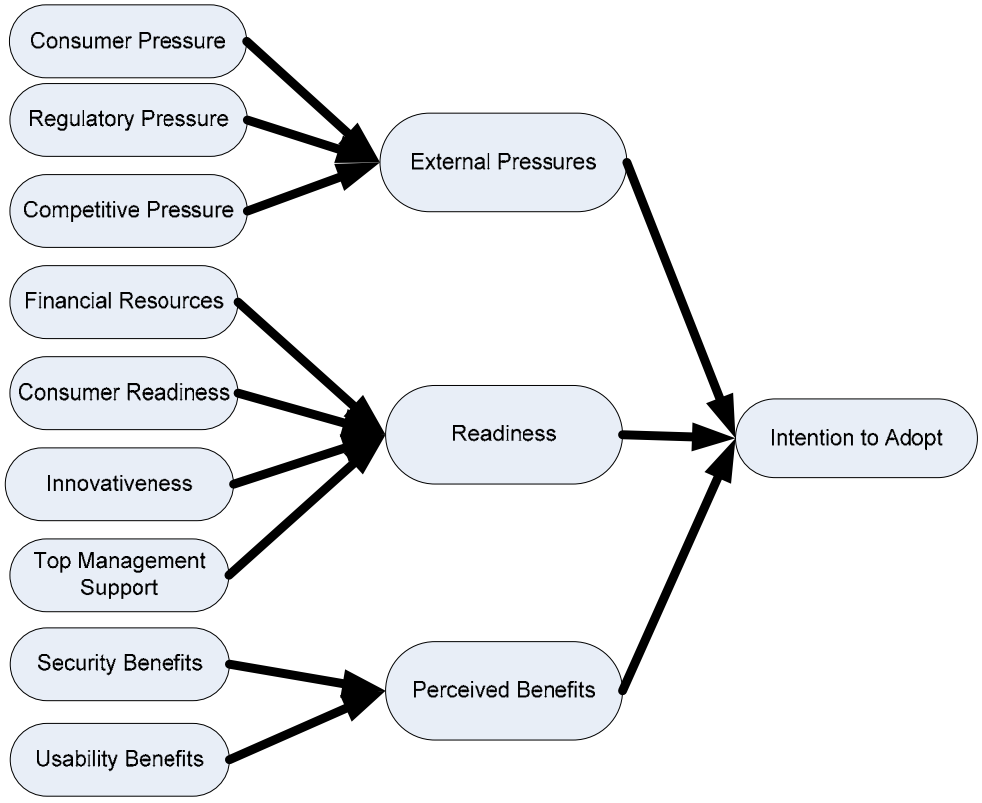

Figure 1, Organizational Adoption Model (adapted from Chwelos, Benbasat, and Dexter, 2001)

3.1.1 Analysis of Factors

As displayed in the research model, this study has identified that these particular factors have been found to be significant in prior research. In adapting the Chwelos et al. (2001) model, sub-factors that are more applicable to the financial industry have been added based on additional research as well (see Table 2). The following section describes each main factor and how the corresponding sub-factors relate.

Table 2. *Summary of the current adoption factors in the study*

Factors in the current study	**Factors in prior studies**	**Source**
External Pressure	External Pressure	Chwelos et al. (2001)
	External Pressure	Grandon & Pearson (2004)
	External Pressure	Iacovou et al. (1995)
	External Pressure	Tsikriktsis et al. (2004)
	Competitive Pressure	Srinivasan et al. (2002)
	Competitive Pressure	Ramamurthy et al. (1999)
Readiness	Readiness	Chwelos et al. (2001)
	Organizational Readiness	Grandon & Pearson (2004)
	Organizational Readiness	Iacovou et al. (1995)
	Organizational Innovativeness	Srinivasan et al. (2002)
	Organizational Innovativeness	Deshpande et al. (1993)
	Organizational Innovativeness	Frambach & Schillewaert (2002)
	Organizational Innovativeness	Subramanian & Nilakanta (1996)
	Internal Management Support	Ramamurthy et al. (1999)
	Top Management Advocacy	Srinivasan et al. (2002)
	Managerial Encouragement	Leonard-Barton & Deschamps (1988)
	Financial Resources	Chwelos et al. (2001)
	Perceived Costs	Premkumar et al. (1994)
	Partner Readiness	Chwelos et al. (2001)
Perceived Benefits	Perceived Benefits	Chwelos et al. (2001)
	Perceived Benefits	Iacovou et al. (1995)
	Anticipated Benefits	Tsikriktsis et al. (2004)
	Expected Benefits	Ramamurthy et al. (1999)
	Relative advantage	Premkumar et al. (1994)

3.1.1.1 External Pressures

In the review of predictors, linkages and biases in IT adoption research by Jeyaraj et al. (2006), External Pressures was found to be one of the best predictors of IT adoption by organizations. In the case of this research study, the factor for external pressure asks the following question: What is the perceived amount of influence from consumers, regulators, and the competition in relation to the pressure to adopt? Organizations that are successful carefully listen to the requests of their consumers and implement those requests that also satisfy the requirements of regulatory mandates and competitive pressures.

H1: *Higher external pressure will lead to greater intent to adopt biometric authentication*. If enough consumers ask for this technology, and other organizations begin implementing it, there will be a drive to adopt.

3.1.1.2 Readiness

There are four sub-factors that present the readiness factor: financial resources, consumer readiness, innovativeness, and top management support. In regards to financial resources, a study by Premkumar, Ramamurthy, and Nilakanta (1994) measured cost by analyzing the perceived cost relative to implementing an innovative technology, such as EDI. Additionally, a study by Subramanian and Nilakanta (1996) used the analysis of past implementations as a measurement of an organization's innovativeness level. These sub-factors encompass the organization's health as to whether or not it is in a position to adopt a new technology. This factor asks such questions as:

- What amount of financial resources is available for adoption?
- Do your members accept new technologies?

- Do you perceive your organization to be innovative?
- Do you traditionally have top management support when adopting a new technology?

The hypothesis for this factor is simply the following:

H2: *Higher readiness will lead to greater intent to adopt biometric authentication.*

3.1.1.3 Perceived Benefits

Iacovou et al. (1995) describe perceived benefits as an organization's level of recognition of the relative advantage that the new technology will give it. The focus of this factor is to study the significance of the perceived benefits of biometric technology in credit unions in relation to the intent to adopt. The five areas of benefits that were chosen for this study were:

- Enhanced ability to compete
- Improved accuracy of authentication
- Reduced operating costs
- Increase in member account security
- Decrease in member transaction time
- Member ease of use

The hypothesis for this factor states:

H3: *Higher perceived benefits will lead to a greater intent to adopt biometric authentication*.

CHAPTER 4. METHODS AND PROCEDURES

The following section details the process in which the research model progressed into a survey instrument. It was then disseminated to a group of credit unions for their participation in the study. The responses where collected via an online survey, and subsequently analyzed.

4.1 Instrument Development

. The survey instrument was developed based on the factors of the research model, and was tailored to the terminology used in the credit union industry. Most questions used a 7 point scale (1= Low to 7=High) with an optional "Don't Know" selection, with the exception of the intention to adopt section that was translated into a seventy point scale for analysis purposes. Each sub-factor had a set of questions, and then further grouped by the relating main factor.

4.1.1 External Pressure Survey Section

The section for external pressure was comprised of items that asked the participant to select the amount of pressure that was felt from members (credit union consumers), government and competitors. These scales are similar to prior research (Chwelos et al., 2001; Grandon & Pearson, 2004; Iacovou et al., 1995; Tsikriktsis et al., 2004; Srinivasan et al., 2002), and are adapted to the credit union industry. The items pertaining to consumer pressure relate to the push that organizations face when their consumers demand a particular product or service. Consequently, these questions relate to a consumer's desire to have biometric authentication available as a means of added protection against theft. The item

pertaining to regulatory pressure relates to the previously mentioned FDIC report (2004) in which the government is encouraging all financial institutions to increase in the level of security by the end of 2006. While the credit union industry is a cooperative environment, there is pressure from within the industry to stay competitive in the market. For example, there is competitiveness within the credit union industry to stay competitive with the banking industry, and to do this, credit unions are encouraged to pull resources together for the development of new technology that may not be possible to fund by one credit union alone.

External Pressures		
CP1	Consumer Pressure	Please rate the amount of influence your credit union members have in your organization's decision to adopt biometrics as an authentication solution. (No Influence = 1 to Strong Influence = 7)
CP2	Consumer Pressure	For each item, please allocate the percentage of encouragement or pressure put on your organization by your credit union members. (Answer should total 100%) **Promise**. Members have made promises of increasing their financial business with your credit union if biometrics are adopted **Request**. Members have asked that your credit union adopt biometrics **No encouragement or pressure**. Members have expressed no opinions on biometric authentication. **Concern**. Members have voiced concerns over the use of biometric authentication adoption in your credit union. **Threat**. Members have made threats to discontinue their relationship with the credit union if biometric authentication is adopted.
RP1	Regulatory Pressure	Please rate your perceptions of the amount of pressure as shown that you expect government regulators to place on your organization to adopt biometrics now or in the next three (3) years for financial services such as kiosks, safety deposit box access, and teller line transactions. (No Pressure at all = 1 to Extreme Pressure = 7)
CPP1	Competitive Pressure	Please rate your perceptions of the amount of pressure placed on your organization by other credit unions to adopt biometrics. (No Pressure at all = 1 to Extreme Pressure = 7)
CPP2	Competitive Pressure	Please rate your perceptions of the amount of pressure placed on your organization by other financial institutions (excluding credit unions) to adopt biometrics. (No Pressure at all = 1 to Extreme Pressure = 7)

4.1.2 Readiness Survey Section

The factor of readiness encompasses the level at which the organization is ready to implement a new technology (Chwelos et al., 2001; Grandon & Pearson, 2004; Iacovou et al., 1995). In the current study, there are four sub-factors that make up the main factor of readiness: financial resources, consumer readiness, innovativeness, and top management support. The item pertaining to innovativeness measures how the organization perceives itself when implementing new products and services in relation to other competitors. Innovativeness has been found to be a significant factor when measured as an influencing factor in adoption (Srinivasan et al., 2002; Deshpande et al., 1993; Frambach & Schillewaert, 2002). In any organization if it is perceived that there is little top management support for a particular project, it will more than likely fail. So the purpose of measuring top management support is to understand the level at which the organization perceives that it has enough support to adopt a new technology implementation. The same can be said for the financial resources item of the survey. Finally, the item pertaining to consumer readiness is based on prior implementations that can be found in the credit union industry. The rate at which prior implementations progressed can be an indicator of how likely an organization will proceed with subsequent technology adoptions.

Readiness		
IN1_1-IN1_4	Innovativeness	When introducing new products and services, please rate how your credit union compares to other credit unions. (Strongly Disagree = 1 to Strongly Agree = 7) 1. We are first to market with innovative new products and services 2. We are first to develop a new process technology 3. We are first to recognize and develop new markets 4. We are at the leading edge of technological innovation

Readiness (cont)		
TMS1_1-TMS1_4	Top Management Support	Please rate the advocacy of your top management where it pertains to the deployment of new technologies. (Strongly Disagree = 1 to Strongly Agree = 7) 1. Top managers repeatedly tell managers that the credit union must gear up to meet changing technology trends 2. Top managers always make an effort to convince managers of the benefits of a new technology 3. Top managers always encourage employees to develop and implement new technologies 4. Top managers in this organization are frequently the most ardent champions of new technologies
FR1	Financial Resources	In the context of your organization's overall Information Systems budget, how significant would the financial cost be in developing and implementing biometrics as an additional level of authentication? (Not at all Significant = 1 to Extremely Significant = 7)
FR2	Financial Resources	Approximately how many members have accounts in your credit union?
FR3	Financial Resources	What is the asset size of your credit union?
CR1_1-CR1_4	Consumer Readiness	Please rate how receptive your members were to accepting technology deployments within your organization. (Low Acceptance = 1 to High Acceptance = 7) 1. Online Banking 2. Electronic Bill Pay 3. Electronic Statements 4. Debit Cards

4.1.3 Perceived Benefits Survey Section

The following perceived benefits of biometric authentication technology were listed for the participants to rate as to whether the benefit was not at all important to the organization to being perceived as extremely important to the organization. The perceived benefits of a new technology are an indication of the relative advantage an organization

would receive by adopting it (Iacovou et al., 1995). For a credit union, the importance of the perceived benefits should be an indicator of how likely the intention to adopt will be. As it will be noted in the results and analysis section, after the survey was given there was a split in the perceived benefits. It was found that the benefits needed to be further grouped into security and usability due to the context of the questions.

Perceived Benefits		
PB1_1-PB1_6	Perceived Benefits	Please rate the importance of achieving each of the following benefits of biometrics in terms of your organization's decision to adopt biometrics. (Not at all Important = 1 to Extremely Important = 7) 1. Enhanced Ability to Compete 2. Improved Accuracy of Authentication 3. Reduced Operating Costs 4. Increase in Member Account Security 5. Decrease in Member Transaction Time 6. Member Ease of Use

4.1.4 Intention to Adopt Survey Section

The dependent variable for this study is the intention to adopt biometric authentication technology. These items simply measure how likely or at what stage is each organization at when it comes to adopting biometric authentication technology. The following items were used to analyze the research model and test for significance. Due to the difference in the scales, the factors were weighted on a 70 point scale.

Intention to Adopt		
IA1	Intention to Adopt	At what stage of biometric system development is your organization currently engaged? * Not currently developing a biometric authentication solution (Weight = 10)

		* Planning (Weight = 30) * Pilot testing (Weight = 50) * Currently have a biometric solution in production (Weight = 70)
IA2	Intention to Adopt	What is the likelihood that your organization intends to adopt biometrics as an additional level of authentication in the next six months? (Not at all likely = 10 to Extremely likely = 70)
IA3	Intention to Adopt	How soon do you anticipate that your organization will adopt a biometric solution? * Less than 6 months (Weight = 70) * 6 months to 1 year (Weight = 58) * 1 year to 2 years (Weight = 46) * 2 to 3 years (Weight = 34) * More than 3 years (Weight = 22) * Do not anticipate ever adopting biometrics (Weight = 10)
IA4	Intention to Adopt	Based on your previous response, how confident are you in the intent to adopt a biometric solution in your organization? _____%

4.2 Subjects

The target industry for this study was the credit union industry. There are currently credit unions, such as Purdue Employees Federal Credit Union and Technology Credit Union, which already offer biometric technology as a means of authentication to their membership. It has become an annual topic of conversation at the CUNA Technology Council Summit, so it was fitting to survey the CUNA Technology Council Members on each organization's plans to adopt biometric technology as a means of secure authentication for its membership base. It has also become an important topic of conversation in the financial industry as a whole due to the FFIEC report in 2005 stating that all financial institutions must improve their security measures by end of 2006 in order to control the amount of fraud that is building each day (FFIEC, 2004).

4.3 Data Collection

As described above, a survey instrument was created based on the factors presented in the model and distributed to 425 credit unions via email in May of 2006 which directed the participants to an online survey. The 425 credit unions were listed as members of the CUNA Technology Council at the time of distribution. A second reminder was sent to the same set of council members in July of 2006 via email, and then again in August of 2006 at the CUNA Technology Council Summit a paper survey was handed out to attendees (attendees were specifically asked if they had filled the survey out online and a paper survey was not given to those who had already completed the survey). A copy of the survey can be found in the Appendix of this paper.

A total of 116 responses were received; however, only 79 were usable based on the completeness of each submitted survey. This results in a response rate of 18.6%. This was calculated by adding the 21 paper surveys to the already usable 58 surveys that were completed online and dividing by the 425 members of the CUNA Technology Council. The attendees of the CUNA Technology Council Summit must be members, thus those that filled out the 21 paper surveys received the emails in May and July of 2006 but chose not to complete the survey online at that time. Possible reasons for this response rate may have been due to the topic as it is a new technology, the method in which the survey was disseminated, and the time in which the survey request was made (employee summer vacations).

CHAPTER 5. RESULTS

5.1 Data Preparation

Once all of the surveys were collected, it was important to cleanse the data and code the variables properly. First, any participant that chose the option “Don’t Know” as well as any surveys that had blank responses was removed from the data to be analyzed due to the fact that it was not considered a completed survey. Second, the financial resources scale was cut to just the first question, due to the compatibility of the questions, and then it was reversed to comply with the rest of the Readiness factor. Third, the intention to adopt scales was weighted to a larger scale range for compatibility purposes, and the fourth question in the section was dropped from the analysis. Finally, the data were then analyzed by using statistical software to determine significance of the model.

5.2 Statistical Analysis

Based on the data obtained, a series of statistical methodologies were selected for analysis such as a descriptive statistical analysis, factor analysis, reliability analysis, and a multiple regression analysis. The descriptive statistical analysis was primarily used to describe the basic elements of the data in this study, while the factor analysis and reliability analysis were used to test whether each of the items and subsequent sub-factors were a good fit in the model. The multiple regression analysis was simply used to understand more about the relationship between the independent variables and the dependent variable (the intention to adoption biometric technology).

The first investigation performed on the survey data consisted of a descriptive statistical analysis of all items used from the survey instrument (see Appendix B) and of the three main aggregated factors in the research model (see Table 3). The examination displays the difference in variability between the aggregated variables of the model.

Table 3. Aggregated Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Dev.
External Pressure	79	1.0	4.9	3.106	.9187
Readiness	79	3.00	6.56	4.6772	.73764
PB_Security	79	2	7	6.23	1.009
PB_Usability	79	2.0	7.0	5.085	1.1194
* Based on a 7 point scale (1 = Low to 7 = High).					

5.2.1 Principal Components Analysis

A principal components analysis was performed to identify the maximum variance from all of the items. As displayed in Table 4, a varimax rotation method was used. Using the Kaiser Eigenvalues criterion, eight components were above the 1.0 rule with a 21.815% explanation of the variance in all items. Within the rotated matrix, top management support (TMS1_1-TMS1_4) and innovativeness (IN1-IN4) loaded quite well while a few of the factors did not load cleanly. Two of the factors, financial resources (FR1_Rev) and regulatory pressure (RP1), are single factors from the data. It is interesting to note that the regulatory pressure factor did load with the competitive pressure factors (CPP1 and CPP2), and they are all sub-factors of External Pressure. Alternatively, the factors for consumer pressure (CP1 and CP2) did not load cleanly, and they are also part of External Pressure.

Overall, results indicate that there is moderate convergent validity as well as moderate discriminant validity for the items.

Table 4. Rotated Component Matrix

	Component							
	1	2	3	4	5	6	7	8
TMS1_2	**.906**	.096	.062	.066	-.038	.143	.102	-.055
TMS1_3	**.892**	.232	-.008	.103	.101	.009	.034	-.027
TMS1_1	**.875**	.217	-.004	.058	-.062	-.032	.028	-.102
TMS1_4	**.846**	.281	.068	.120	-.030	.021	.059	.035
IN1_3	.155	**.859**	.015	.098	.066	-.027	.017	-.122
IN1_1	.239	**.838**	.242	.092	-.036	.072	.106	.114
IN1_2	.227	**.820**	.172	.078	.013	-.032	.065	.125
IN1_4	.289	**.797**	.207	.013	-.097	.187	.029	.066
IA3	-.026	.153	**.841**	.044	.165	.072	-.013	.071
IA2	.058	.226	**.826**	.045	.206	-.102	.054	-.012
IA1	.115	.233	**.781**	.148	.083	.050	-.117	.161
IA4	.054	.103	**.661**	-.143	.047	.072	.130	-.466
FR1_Rev	-.097	-.225	**.556**	.166	-.441	-.002	.123	-.176
CR1_2	-.004	.096	-.022	**.894**	.087	.105	-.050	.050
CR1_1	.115	.058	.115	**.834**	-.046	-.116	.111	-.081
CR1_3	.264	.077	.066	**.725**	.208	.039	.091	.329
CR1_4	.188	.169	.198	**.508**	.001	-.096	-.074	-.496
CPP2	-.012	-.063	.060	.146	**.863**	.059	.010	.091
CPP1	.015	-.082	.223	.042	**.853**	.041	-.105	.123
RP1	-.151	.120	.123	.034	**.626**	-.144	.244	-.382
PB1_3	.091	-.059	-.043	-.066	-.004	**.834**	.210	.016
PB1_5	.129	.120	.214	.036	.068	**.762**	.053	-.057
PB1_6	-.160	.131	-.104	.058	-.130	**.585**	.347	-.097
PB1_1	.116	.035	.023	-.143	.270	**.481**	.411	.129
CP1	.204	.160	.153	-.310	.315	**-.403**	.080	.290
PB1_4	.083	.025	-.057	.054	.014	.243	**.879**	.038
PB1_2	.112	.113	.113	.058	-.031	.205	**.876**	.004
CP2	-.158	.295	.095	.166	.150	-.164	.094	**.701**

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 8 iterations.

Based on the item analysis and groupings found in the rotated component matrix, a reliability analysis was assessed on each of the hypothesized factors using Cronbach's alpha. Table 5 lists each of the sub-factors that include more than one item. Based on the

acceptable alpha level found in field research (Hair et al., 1998), the values range from .729 to .939, with the exception of consumer pressure with a alpha of .265. The two items in consumer pressure are conclusively not convergent.

Upon further review of these two items in the survey instrument, the first item (CP1) rates the perceive amount of influence that a member has on the credit union's decision to adopt biometric technology. The second item (CP2) asks the participant to allocate the percentage of member encouragement or pressure put on the organization to adopt biometric technology. The majority of participants placed 100% in the section labeled "No encouragement or pressure" whereas there was more variability in the first item. Based on the compatibility issue, it can be concluded that even though members may influence decision making, the members are not asking for this technology. Consequently, the two items (CP1 and CP2) are dropped from any further analysis.

Table 5. Reliability Statistics

Factor	Cronbach's Alpha	N of Items
Top Management Support	.939	4
Innovativeness	.906	4
Competitive Pressure	.899	2
Security Benefits	.870	2
Intention to Adopt	.834	4
Consumer Readiness	.792	4
Usability Benefits	.729	4
Consumer Pressure	.265	2

5.2.3 Multiple Linear Regression Examination

The original research model was designed to determine if the main factors of *External Pressure, Readiness, and Perceived Benefits* are significant indicators of the intention to adopt biometric authentication technology. Based on the regression analysis, the results of

the study demonstrate that the model has an overall fit, but that there are specific significant factors that contribute to the overall fit of the main factors. In the case of the model summary in Table 6, 31.9% of the variance in the intention to adopt is explained by the model (Perceived Benefits, External Pressure and Readiness).

Table 6. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.588(a)	.345	**.319**	13.865	.345	13.189	3	75	.000

a Predictors: (Constant), Perceived Benefits, External Pressure, Readiness

The coefficient analysis in Table 7 reveals that External Pressure and Readiness are significant predictors at the $p < .05$ level of the intention to adopt biometrics; however, Perceived Benefits have no significant value in the relationship.

Table 7. Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-29.115	13.207		-2.205	.031
	External Pressure	4.529	1.321	.322	3.429	.001
	Readiness	12.109	2.179	.532	5.558	.000
	Perceived Benefits	-.858	1.559	-.052	-.550	.584

a Dependent Variable: Intent to Adopt

As in the Chwelos et al. (2001) study, the following section details the sub-factors that were most influential in each of the main factors of the model. The analysis provides a clearer understanding of what aspects in each main factor may be more prominent than others when influencing the intent to adopt biometric authentication systems.

By breaking out the sub-factors and analyzing them in relation to the dependent variable of adoption intention, the following results are found in Table 8. By disaggregating

the factors into sub-factors, the amount of variance explained by the model improves dramatically. In the case of the model summary, 43.7% of the variance in the intention to adopt is explained by the model (Usability Perceived Benefits, Regulatory Pressure, Customer Readiness, Financial Resources, Top Management Support, Competitive Pressure, Security Perceived Benefits and Innovativeness). As stated before, a decision was made to remove consumer pressure due to the poor reliability analysis results.

Table 8. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	Df1	df2	Sig. F Change
1	.704(a)	.495	**.437**	12.605	.495	8.578	8	70	.000

a Predictors: (Constant), Perceived Benefits - Usability, Regulatory Pressure, Consumer Readiness, Financial Readiness, Top Management Support, Competitive Pressure, Perceived Benefits - Security, Innovativeness

By breaking out the sub-factors, the impact of each sub-factor is revealed in Table 9. There is significance with Competitive Pressure, Innovativeness, and Financial Resources.

Table 9. Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-11.133	13.070		-.852	.397
	Regulatory Pressure	.951	.962	.092	.989	.326
	Competitive Pressure	4.601	1.198	.363	3.841	**.000**
	Innovativeness	6.290	1.296	.480	4.853	**.000**
	Top Management Support	.176	1.351	.013	.130	.897
	Financial Resources	5.703	1.066	.482	5.349	**.000**
	Consumer Readiness	-.467	1.744	-.025	-.268	.790
	PB-Security	-2.977	1.686	-.179	-1.765	.082
	PB-Usability	1.018	1.491	.068	.683	.497

a Dependent Variable: Intent to Adopt

These sub-factors are the primary contributors in adding explanatory power to the primary factors. For instance, Top Management Support and Customer Readiness have no significance, but the Financial Resources and Innovativeness are significant and, when aggregated, *carry* the other two factors.

CHAPTER 6. SUMMARY AND DISCUSSION

The results of the study demonstrate that the model has an overall fit, but that there are specific significant factors that contribute to the overall fit of the primary factors. When reviewing the main factors in the model in relation to the measured predictor variables of *Intention to Adopt*, *Readiness* and *External Pressures*, the results show that these two variables are significant while the variable of *Perceived Benefits* is not. The results suggest that more explanatory power exists in these data when we focus our analysis to the sub-factors. The sub-factor Competitive Pressure adds the most explanatory power and appears to be what is making the primary factor External Pressure significantly related to the intention to adopt. For the factor Readiness, the sub-factors Financial Resources and Innovativeness offer most of the explanatory power.

The results of this model suggest that these sub-factors have a significant explanatory power in that the probability of adoption of biometrics could be predicted almost 44% of the time. The results indicate that the intent to adopt biometric authentication is driven by competitiveness and finances and not by the perceived benefits within the credit union industry. In a review of the original three hypotheses of the research model, H1 and H2 are supported whereas H3 was not.

H1: *Higher external pressure will lead to greater intent to adopt biometric authentication.*	**Supported**
H2: *Higher readiness will lead to greater intent to adopt biometric authentication.*	**Supported**
H3: *Higher perceived benefits will lead to a greater intent to adopt biometric authentication.*	**Not Supported**

6.2 Implications

On December 14, 2004 the FDIC published a report titled *Putting an End to Account-Hijacking Identity Theft.* The purpose of this study was to increase the level of awareness in financial institutions to the threat of identity theft. The study was also an educational document on the methods available to increase security and thwart theft. Then on October 12, 2005, the FFIEC published a report titled *Authentication in an Internet Banking Environment* which strongly encouraged all financial institutions to select a method of two-factor authentication for their online banking systems by the end of 2006. Possible methods for accomplishing this task referenced the FDIC study as a resource. One method described in both reports was biometric authentication. This was surprising since the use of biometric authentication technology has yet to become widely accepted in the United States. These two reports are the basis to why this study is important due to the fact that the government is suggesting that this technology is a valid deterrent against theft. Even though the focus of the FFIEC report pertains to the online banking environment, it just as important to secure a consumer's financial accounts from within a branch office. Although the sub-factor of regulatory pressure was not found to be significant in the results of this study, this may be a situation where the participants do not recognize biometrics as the most popular choice for additional authentication based on the other options suggested within the government reports.

One question based on the results is "Do organizations find the biometric system information presented in the government reports to be useful?" As well as, "Is the information presented in such a way that it relates to the daily operations of a financial institution?" The findings from this study suggest that it will take more practitioner based education on the benefits of biometrics for decision makers to accept it. Biometric

authentication technology is still in an infancy stage where it is considered more of a new and innovative technology rather than a practical solution for an organization. This is also why the expected outcome in the research study was that innovative credit unions would be more likely to adopt biometrics. This is because early adopters of new technology discover the benefits as well as hazards involved, and can influence any subsequent implementations by other credit unions.

The sub-factor of financial resources is significant to the readiness of the organization much like the influence of the innovativeness sub-factor. An organization must have the resources available and the willingness to implement a technology that has not been widely utilized when the fact is that the business plan may fail. As Jain et al. (2004) pointed out in their study of biometric technology implementations, there are barriers that are still of great concern such as accuracy, scale, security and privacy. This is evident in the results of this study as those barriers have financial implications that must be planned for before deciding to adopt a biometric system.

The most surprising result of the study was the sub-factor relating to competitiveness and how it influenced the intent to adopt. This result is similar to what Tsikriktsis et al. (2004) called the “bandwagon” effect. In this situation, the pressure to keep up with competitors is significant even when the perceived benefits are not influencing the intention to adopt. This is an indicator of why there is a high failure rate when it comes to new implementations due to a lack of strategic planning and understanding of what the technology is rather than keeping up with a competitor.

Overall the results of the model are indicative of the situations that organizations face when making business decisions whether or not to adopt a new technology. Not all of the

sub-factors were significant, but biometric authentication technology is new and not widely accepted by consumers yet. This situation may very well change in the next five years, and the results of this research model would possibly uncover different significant influencers, such as benefits or consumer pressure due to identity theft issues.

6.2 Limitations

There are a few limitations of this study that are important to consider. First, the participants of this study represent one area of industry which is credit unions and they do not reflect all of the financial institution industry. Second, the credit union participants of this study are members of a Technology Council and therefore may be more innovative by nature. Finally, the number of responses that were gathered was low and thus may not be a true representative of the entire credit union industry.

6.3 Future Research

The purpose of this study was to better understand the intention of an organization to adoption biometric authentication technology, specifically credit unions. The same study could be performed on a larger audience of credit unions, as well as financial institutions as a whole. The use of biometric technology is growing with the increase of identity theft and account fraud. Organizations are looking for alternatives that will be secure, safe and customer friendly, and this type of study may become more valuable as more environments begin to accept biometric technologies.

6.4 Conclusion

The goal of this study is to better understand an organization's view on the adoption of a new technology such as biometric authentication. Biometric technology is still in an infancy phase in relation to implementations throughout any industry. There is apprehension by many due to level of education and awareness of society on the qualities of this technology. On the other hand, those that voice concerns are the reason why these innovative technologies improve. By asking questions and finding faults, those that create the new technology that we come to expect in society can make it better. One problem is that organizations must take a stronger stance against fraud and identity theft as it is raging out of control. Biometrics may not be the immediate answer, but by increasing the awareness of the possibilities, something that is viable will come forward.

The interesting outcome of this study was that based on the results, competition is a more important factor in adopting biometrics than the perceived benefits. This could mean that keeping up with the competition is more important the actual benefits of this technology. Or maybe the participants at this point do not see a significant benefit to adopting this type of technology. An increase of education in the benefits of biometrics may assist in a greater enrollment rate, and while perceived benefits may not be significant, a better understanding of the technology will change the outlook of the benefits.

APPENDIX A. SURVEY INSTRUMENT

Survey Instructions: As you answer each of the survey questions, please consider the context of the study as it relates to the adoption of biometrics as an additional level of authentication in financial services (such as kiosks, safety deposit box access, and teller line transactions) for your organization.

		No Influence			Moderate Influence			Strong Influence	Don't Know
1.	Please rate the amount of influence your credit union members have in your organization's decision to adopt biometrics as an authentication solution.	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

2. For each item, please allocate the percentage of encouragement or pressure put on your organization by your credit union members. (Answer should total 100%)

	Promise. Members have made promises of increasing their financial business with your credit union if biometrics are adopted
	Request. Members have asked that your credit union adopt biometrics
	No encouragement or pressure. Members have expressed no opinions on biometric authentication.
	Concern. Members have voiced concerns over the use of biometric authentication adoption in your credit union.
	Threat. Members have made threats to discontinue their relationship with the credit union if biometric authentication is adopted.

		No Pressure at all			Some Pressure			Extreme Pressure	Don't Know
3.	Please rate your perceptions of the amount of pressure as shown that you expect government regulators to place on your organization to adopt biometrics now or in the next three (3) years for financial services such as kiosks, safety deposit box access, and teller line transactions.	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
4.	Please rate your perceptions of the amount of pressure placed on your organization by other credit unions to adopt biometrics.	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
5.	Please rate your perceptions of the amount of pressure placed on your organization by other financial institutions (excluding credit unions) to adopt biometrics.	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

6. When introducing new products and services, please rate how your credit union compares to other credit unions.

	Strongly Disagree			Neutral			Strongly Agree	Don't Know
We are first to market with innovative new products and services	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
We are first to develop a new process technology	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
We are first to recognize and develop new markets	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
We are at the leading edge of technological innovation	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

7. Please rate the advocacy of your top management where it pertains to the deployment of new technologies.

	Strongly Disagree			Neutral			Strongly Agree	Don't Know
Top managers repeatedly tell managers that the credit union must gear up to meet changing technology trends	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Top managers always make an effort to convince managers of the benefits of a new technology	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Top managers always encourage employees to develop and implement new technologies	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Top managers in this organization are frequently the most ardent champions of new technologies	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

		Not at all Significant					Moderately Significant	Extremely Significant	Don't Know
8.	In the context of your organization's overall Information Systems budget, how significant would the financial cost be in developing and implementing biometrics as an additional level of authentication?	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

9. Approximately how many members have accounts in your credit union? _____

10. What is the asset size of your credit union? _____

11. Please rate how receptive your members were to accepting technology deployments within your organization.

	Low Acceptance			Neutral			High Acceptance	Don't Know
Online Banking	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Electronic Bill Pay	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Electronic Statements	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Debit Cards	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

12. At what stage of biometric system development is your organization currently engaged?

- ❒ Not currently developing a biometric authentication solution
- ❒ Planning
- ❒ Pilot testing
- ❒ Currently have a biometric solution in production

		Not at all likely to adopt biometrics			Moderate likelihood to adopt biometrics		Extremely likely to adopt biometrics	Don't Know
13.	What is the likelihood that your organization intends to adopt biometrics as an additional level of authentication in the next six months?	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

14. How soon do you anticipate that your organization will adopt a biometric solution?

- ❒ Less than 6 months
- ❒ 6 months to 1 year
- ❒ 1 year to 2 years
- ❒ 2 to 3 years
- ❒ More than 3 years
- ❒ Do not anticipate ever adopting biometrics

15. Based on your previous response, how confident are you in the intent to adopt a biometric solution in your organization? _____%

16. Please rate the importance of achieving each of the following benefits of biometrics in terms of your organization's decision to adopt biometrics.

	Not at all important			Moderately Important			Extremely Important	Don't Know
Enhanced Ability to Compete	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Improved Accuracy of Authentication	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Reduced Operating Costs	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Increase in Member Account Security	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Decrease in Member Transaction Time	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒
Member Ease of Use	1 ❒	2 ❒	3 ❒	4 ❒	5 ❒	6 ❒	7 ❒	X ❒

APPENDIX B. DESCRIPTIVE STATISTICAL ANALYSIS

Descriptive Statistics

	N	Range	Minimum	Maximum	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
CP1	79	6	1	7	4.58	.202	1.795	3.221
CP2	79	3	1	4	1.51	.082	.732	.536
RP1	79	6	1	7	4.11	.183	1.625	2.641
CPP1	79	5	1	6	2.53	.153	1.357	1.842
CPP2	79	5	1	6	2.80	.161	1.427	2.035
IN1_1	79	6	1	7	4.73	.166	1.474	2.172
IN1_2	79	6	1	7	4.38	.159	1.417	2.008
IN1_3	79	6	1	7	4.49	.145	1.290	1.663
IN1_4	79	6	1	7	4.62	.181	1.612	2.598
TMS1_1	79	5	2	7	5.44	.149	1.328	1.763
TMS1_2	79	6	1	7	5.43	.145	1.288	1.659
TMS1_3	79	6	1	7	5.30	.153	1.362	1.855
TMS1_4	79	6	1	7	5.13	.159	1.418	2.009
FR1_Rev	79	6	1	7	3.22	.160	1.420	2.017
CR1_1	79	4	3	7	5.80	.120	1.067	1.138
CR1_2	79	5	2	7	5.14	.149	1.328	1.762
CR1_3	79	6	1	7	5.01	.149	1.325	1.756
CR1_4	79	2	5	7	6.49	.078	.696	.484
IA1	79	60	10	70	28.99	2.414	21.459	460.500
IA2	79	60	10	70	31.65	2.296	20.408	416.488
IA3	79	60	10	70	44.63	1.716	15.250	232.569
PB1_1	79	6	1	7	4.41	.182	1.613	2.603
PB1_2	79	5	2	7	6.06	.123	1.090	1.188
PB1_3	79	5	2	7	4.92	.170	1.509	2.276
PB1_4	79	5	2	7	6.39	.119	1.055	1.113
PB1_5	79	6	1	7	5.06	.163	1.453	2.111
PB1_6	79	6	1	7	5.95	.163	1.449	2.100
Valid N (listwise)	79							

* All items are based on a 7 point scale (1 = Low to 7 = High).

BIBLIOGRAPHY

Agarwal, Ritu and Prasad, Jayesh. The antecedents and consequents of user perceptions in information technology adoption. *Decision Support Systems*, 22, (1998), 15-29.

Ahmed, Fawad and Siyal, M.Y. A novel approach for regenerating a private key using password, fingerprint and smart card. *Information Management & Computer Security*, 13, 1 (2005), 39-54.

Alterman, A. A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology*, 5, 3 (2003), 139-150.

Better Business Bureau. 2006 Identity Fraud Survey Report. Consumer Report, January 2006. [Online]. Available: http://www.javelinstrategy.com/research.

Bolle, R.M.; Connell, J.H.; Pankanti, S.; Ratha, N.K.; and Senior, A.W. *Guide to biometrics*. New York: Springer-Verlag, 2004.

Breckenridge, K. The biometric state: The promise and peril of digital government in the new south Africa. *Journal of Southern African Studies*, 31, 2 (2005), 267-282.

Chandra, Akhilesh and Calderon, Thomas. Challenges and constraints to the diffusion of biometrics in information systems. *Commun. ACM*, 48, 12 (2005), 101-106.

Chwelos, P.; Benbasat, Izak; and Dexter, Albert S. Research report: Empirical test of an EDI adoption model. *Information Systems Research*, 12, 3 (2001), 304.

Coventry, Lynne; De Angeli, Antonella; and Johnson, Graham. Honest it's me! Self service verification. *CHI Workshop on Human-Computer Interaction, Adoption Study and Security Systems*, Fort Lauderdale, FL, ACM Press, New York, NY, April 2003, 1-6.

Coventry, Lynne; De Angeli, Antonella; and Johnson, Graham. Usability and biometric verification at the ATM interface. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, ACM Press, New York, NY, April 2003.

Davis, Fred D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13, 3 (September 1989), 319-340.

Deshpande, Rohit; Farley, John; and Webster, Jr., Frederick. Corporate culture, customer orientation, and innovativeness in Japanese firms: A quadrad analysis. *Journal of Marketing*, 57 (January 1993), 23-27.

Elliott, Stephen; Kukula, Eric P.; and Sickler, Nathan C. The challenges of the environment and the human/biometric device interaction on biometric system performance. *International Workshop on Biometric Technologies – Special Forum on Modeling and Simulation in Biometric Technology*, Calgary, Alberta, Canada, 2004.

Fairhurst, M. C. Document Identity, Authentication and Ownership: The Future of Biometric Verification. *Seventh International Conference on Document Analysis and Recognition (ICDAR'03)*, Edinburgh, Scotland, 3-6 August 2003, pages 1108-1116.

FDIC. Putting an end to account-hijacking identity theft. Tech. Report, December 2004. [Online]. Available: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity theft.pdf.

FFIEC. Authentication in an Internet Banking Environment, October 12, 2005. [Online]. Available: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

Federal Trade Commission. Consumer fraud and identity theft complaint data, January – December 2005. Consumer Report, January 2006. [Online]. Available: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

Frambach, R. T., and Schillewaert, Niels. Organizational innovation adoption: A multi-level framework of determinants and opportunities for future research. *Journal of Business Research*, 55, 2 (2002), 163-176.

Giesen, Lauri. Biometrics: Ready for primetime? *Published by BAI*, 82, 3 (May/June 2006). Available: http://www.bai.org/bankingstrategies/2006-may-june/biometrics/index.asp.

Gopalakrishnan, S. and Damanpour, F. A review of innovation research in economics, sociology and technology management. *Omega, International Journal of Management Science*, 25, 1 (1997), 15-28.

Grandon, E. and Pearson, Michael. Electronic commerce adoption: an empirical study of small and medium US businesses. *Information & Management* , 42, 1(2004), 197 - 216.

Hair, J. F.,Anderson, R. E., Tatham, R. L.&Black, W. C. (1998) in *Multivariate Data Analysis* (Prentice–Hall, Englewood Cliffs, NJ).

Harris, A. J. and Yen, D. C. Biometric authentication: Assuring access to information. *Information Management & Computer Security*, 10, 1 (2002), 12-19.

Heracleous, L., and Wirtz, J. Biometrics: the next frontier in service excellence, productivity and security in the service sector. *Managing Service Quality*, 16, 1 (2006), 12 pages.

Iacovou, Charalambos L.; Benbasat, Izak; and Dexter, Albert S. Electronic data interchange and small organizations: Adoption and impact of technology. *MIS Quarterly*, 19, 4 (1995), 465 - 485.

International Biometric Group. Biometrics Market and Industry Report 2006-2010. January 2006. [Online]. Available: http://www.biometricgroup.com/reports/public/market_report.html.

Jain, A. K. Biometric recognition: How do I know who you are? *Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE 12th*. Kusadasi, Turkey, April 2004, 3-5.

Jain, A. K.; Pankanti, S.; Prabhakar, S.; Hong, L.; and Ross, A. Biometrics: A grand challenge. *17th International Conf. on Pattern Recognition (ICPR'04)*, 2, 2004, 935-942.

James, T.; Pirim, T.; Boswell, K.; Reithel, B.; and Barkhi, R. Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing*, 18, 3 (July – September 2006): 1-24.

Jeyaraj, Anand; Rottman, Joseph; and Lacity, Mary. A review of the predictors, linkages, and biases in IT innovation adoption research. *Journal of Information Technology*, 21, (2006), 1-23.

Jones, MC and Beatty, RC. Towards the development of measures of perceived benefits and compatibility of EDI: a comparative assessment of competing first order factor models. *European Journal of Information Systems*, 7, (1998), 210-220.

Kleist, V.; Riley Jr., R.; Pearson, T. Evaluating Biometrics as Internal Control Solutions to Organizational Risk. *Journal of American Academy of Business, Cambridge*, Hollywood, 6, 2 (2005): 339-343.

Langenderfer, J. and Linnhoff, S. The emergence of biometrics and its effect on consumers. *Journal of Consumer Affairs*, 39, 2 (2005), 314-338.

Leonard-Barton, Dorothy and Deschamps, Isabelle. Managerial influence in the implementation of new technology. *Management Science*, 34, 10 (October 1988), 1252-1265.

Miller, B. Vital signs of identity. *IEEE Spectrum*, 31, 2 (Feb 1994), 22-30.

Moody, J. Public perceptions of biometric devices: The effect of misinformation on acceptance and use. *Journal of Issues in Informing Science and Information Technology*, 1 (2004): 753 - 761.

Moore, Gary C. and Benbasat, Izak. Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research*, 2, 3 (1991), 192- 222.

Mustonen-Ollila, Erja and Lyytinen, Kalle. Why organizations adopt information system process innovations: a longitudinal study using Diffusion of Innovation Theory. *Information Systems Journal*, 13 (2003), 275 – 297.

National Science and Technology Council Subcommittee on Biometrics. Introduction to Biometrics. Technical Reports, accessed June 2006. [Online]. Available: http://www.biometricscatalog.org/NSTCSubcommittee/BiometricsIntro.aspx.

Orr, Bill. Biometric ATMs overseas now, but why not here? *American Bankers Association. ABA Banking Journal*, 98, 6 (2006): 51.

Prabhakar, S.; Pankanti, S.; and Jain, Anil K. Biometric recognition: Security and privacy concerns. *Security & Privacy Magazine, IEEE*, 1, 2 (2003), 33-42.

Premkumar, G.; Ramamurthy, K.; and Nilakanta, Sree. Implementation of electronic data interchange: An innovation diffusion perspective. *Journal of Management Information Systems*, 11, 2 (1994), 157-186.

Ramamurthy, K.; Premkumar, G.; and Crum, Michael. Organizational and interorganizational determinants of EDI diffusion and organizational performance: A causal model. *Journal of Organizational Computing and Electronic Commerce*, 9, 4 (1999), 253-285.

Ratha, N. K.; Connell, J. H.; and Bolle, R. M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40, 3 (2001), 614-634.

Riley Jr , Richard A. and Kleist, Virginia Franke. The biometric technologies business case: a systematic approach. *Information Management & Computer Security*, 13, 2 (2005), 89-105.

Rogers, Everett. *Diffusion of innovations*. New York: Free Press, 2003.

Sanderson, S. and J. H. Erbetta. Authentication for secure environments based on iris scanning technology. *IEE Colloquium on Visual Biometrics*, London, England, (March 2000), 8/1-8/7.

Srinivasan, Raji; Lilien, Gary; and Rangaswamy, Arvind. Technological opportunism and radical technology adoption: An application to e-business. *Journal of Marketing*, 66, 3 (2002), 47 - 60.

Sticha, Paul J., and Ford, J. Patrick. Introduction to biometric technology: Capabilities and applications to the food stamp program. *U.S. Department of Agriculture contract no: FCS 53-3198-6-025*, Arlington, VA: R. Lewis & Co., Inc., December 1999, 1-39.

Subramanian, A. and Nilakanta, S. Organizational innovativeness: Exploring the relationship between organizational determinants of innovation, types of innovations, and the measures of organizational performance. *Omega, International Journal of Management Science*, 24, 6 (1996), 631-647.

Suoranta, Mari and Mattila, Minna. Mobile banking and consumer behavior: New insights into the diffusion pattern. *Journal of Financial Services Marketing*, 8, 4 (June 2004), 354-366.

Taylor, Shirley and Todd, Peter. Understanding information technology usage: A test of competing models. *Information Systems Research*, 6, 2 (June 1995), 144 – 176.

Theofanos, M.; Micheals, R.; Scholtz, J.; Morse, E.; and May, P. Does habituation affect fingerprint quality? *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, Montreal, Quebec, Canada, (April 22-27, 2006), 1427-1432.

Tsikriktsis, Nikos; Lanzolla, Gianvito; and Frohlich, Mark. Adoption of e-processes by service firms: An empirical study of antecedents. *Production and Operations Management*, 13, 3 (2004), 216 - 229.

Venkatesh, Viswanath; Morris, Michael G.; Davis, Gordon B.; and Davis, Fred D. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27, 3 (September 2003), 425-478.

Whisenant, Warren. Using biometrics for sport venue management in a post 9-11 era. *Facilities*, 21, 5/6 (2003), pages 134-141.

Zorkadis, V. and Donos, P. On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security*, 12, 1 (2004), 125-137.