Perceptions of biometric experts on whether or not biometric modalities will combat identity fraud

Galaxy Samson Edo
Capella University

Sherri Nicole Braxton-Lieber
Capella University

ABSTRACT

Electronic-authentication methods, no matter how sophisticated they are in preventing fraud, must be able to identify people to a reasonable degree of certainty before any credentials are assured (Personix, 2006). The examination of the aftermath of the 9/11 terrorist act brought to light the extent to which the use of fraudulent identification is not only a significant component of fraud but also of terrorism. This qualitative study ascertained the perceptions of biometric-industry experts whether or not biometric modalities will combat identity fraud. A qualitative phenomenological research design was applied and interview of biometric industry experts from various geographical locations in the United States were conducted. The result of this study has highlighted the significance of how biometric modalities will combat identity fraud. Furthermore, this study has included the interviewed expert opinions on how biometric identification can augment an important stratum of defense to the total method of identifying a person.

Keywords: identify fraud, identity theft, biometrics, perceptions, experts, fingerprinting, iris identification, keystroke, DNA and voice.

INTRODUCTION

The upsurge in the proliferation of technology globally has substantially influenced the world. A more collaborative and virtual world has surfaced amid use of the Internet and, as a result, has provided organizations and private entities with a host of unsolicited security concerns (Bochkov, Chiem, & Sai, 2007). Consequently, protecting and safeguarding important data, our individuality, and identity have become areas of imperative concern that cannot be ignored (Bochkov et al., 2007). It is important to increase security levels. However, "maintaining and managing access while protecting both the user's identity and the computer's data and systems has become increasingly difficult" (Bochkov et al., 2007, p. 1).

The terrorist acts of September 11, 2001, or 9/11, have exacerbated our security consciousness to the level that law-enforcement officials and national-security agencies have realized that identity fraud and theft are perpetrated as part of more atrocious crimes than have been previously believed. These incidents officially introduced the harsh reality of identity theft as an enabler of terrorist acts. Paul McNulty, a U.S. Attorney for the Eastern District of Virginia, stated "Our whole system depends upon people being who they say they are. False or stolen identities: undermine our system of commerce as well as our national security" (Burton & Davis, 2002, Para. 3).

The terrorist attack of 9/11 has renewed an unprecedented interest in the adoption of biometric modalities for identification authentication. According to the report published by the National Commission on Terrorist Attacks, the events preceding the attacks on the United States have allowed the citizenry to appreciate the significance of airport security screening of passengers flying to and from the United States (as cited in Bochkov et al., 2007). The commission further proposed that seeking to identify terrorist travelers is as formidable a deterrent against terrorism as is targeting their finances. Bochkov et al. (2007) also purported that the United States needs to fuse terrorist travel intelligence, security operations, and law enforcement into a single stratagem to capture terrorists, locate those who help terrorists travel, and restrict terrorist mobility (p. 4).

BACKGROUND

Prior to the promulgation of the Federal Identity Theft and Assumption Deterrence Act of 1998, no standard characterization of what constituted identity theft existed. The advent of this legislation ushered in a blanket definition, allowing law-enforcement officials the flexibility to bring charges against perpetrators (Newman & McNally, 2007).

The term *identity fraud* has progressed to include an assortment of identification-based illegalities, ranging from the time-honored pecuniary crimes that include "loan, mortgage, credit card, commodities and services frauds, to money laundering, trafficking in human beings, stock market manipulation and even breaches of national security or terrorism" (Wilcox & Regan, 2002, p. 4).

There are various definitions of identity theft. Although some definitions are more inclusive, definition of identification "matters because it affects how identity theft is measured and how it can be combated" (Schreft, 2007, p. 6), According to the Identity Theft and Assumption Deterrence Act, identity theft is defined as "the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or

aiding or abetting a crime" (p. 7). These personal-identifying characteristics include name, date of birth, social-security number (SSN), address, telephone number, and bank and credit card numbers (Murphy, 2008; Perl, 2003; Zhao, 2007). In the United States and globally, identity fraud is the most rapidly growing financial crime (Zhao, 2007). Identity frauds such as those used in medical and financial fields are becoming prevalent.

Medical-identity fraud, according to Lafferty (2007), is the "newest frontier in the ever-evolving crime of identity theft" (p. 11) and can be defined as "the inappropriate or unauthorized misrepresentation of individually identifiable health information for the purpose of obtaining access to property or services, which may result in long-lasting harm to an individual interacting with the health care continuum" (Kieke, 2009, p. 51). Medical identity fraud is a growing concern in the healthcare field, and current laws do not adequately address how to effectively prosecute perpetrators who engage in such nefarious activities. Such actions are determined by organizational policies and no federal law-enforcement agency is specifically tasked with the responsibility of investigating and prosecuting this offense because there is no specifically recognized crime of medical-identity fraud (Lafferty, 2007; Schneider, 1997). To combat medical-identify fraud, Lafferty (2007) urged that "health care compliance professionals must lead the way in the effort to combat the future threat of health care fraud through medical identity theft" (p. 11). Kieke (2009) believed that with the insurmountable privacy and security rules that are currently in place, there should be little or no ability to commit medical-identity fraud. To make his point, Kieke cited Rhodes, Director of Practice Leadership for American Health Information Management Association, who claimed,

> most of the problems have to do with the lack of a sound information security plan. While the Health Insurance Portability and Accountability Act (HIPAA) security rules may spell out what a facility needs to do to protect electronic health information and the privacy rules may explain what needs to be done to protect people's privacy, what often fails is the execution of those rules. (Rhodes, as cited in Kieke, 2009, p. 52).

Financial-identity fraud refers to situations when a fraudster has knowingly used personal identifier information of another in commission of a financial-fraud crime. Such crimes include opening an illegal new bank account, opening a new charge account, and defrauding an existing account (Aguilar, 2009). According to Marshall (2007), financial-identify fraud has resulted in crimes estimated at $52.6 billion; the severity of such fraud makes it vital to an organization that an individual doing business with them protect their personal information, as stipulated by the Fair and Accurate Credit Transactions Act (Deybach, 2007).

In the United States and globally, identity fraud is the most rapidly growing financial crime (Zhao, 2007). To compound this assertion, Marshall (2007) cited the Federal Trade Commission report claiming that within the next 5 years most Americans will have fallen a victim of identity theft or fraud. Marshall (2007) cited another report by the Better Business Bureau, stating that 9.3 million Americans became victims of identity theft in 2004 alone. These frauds involved mainly financial and medical-identity fraud. According to the Federal Bureau of Investigation (FBI), an estimated 10 million Americans have had their identities stolen. The costly aftermath is about $50 billion annually (Clarke, 2009).

To this effect, several federal and state laws have been developed to ensure stiff penalties for such illicit activities. In 2004 the Identity Theft Penalty Enhancement Act became federal law with the purpose of establishing penalties for aggravated identity theft (Holtfreter & Holtfreter, 2006). The Fair and Accurate Credit Transactions Act and the Identity Theft Penalty

Enhancement Act help consumers take prescribed actions when they become a victim of identity theft, or even when they suspect they might have become a victim of identity theft. States such as California, New York, and Texas have implemented a *security freeze* to combat such crimes, and are requiring organizations to notify victims of breaches to their personal data (Wilcox & Regan, 2002). Other statutory provisions were enacted to protect the privacy of consumer data in the banking and credit systems by limiting the circumstances under which merchants may access consumer reports, as well as the information that may be included on credit-card and debit-card receipts (Warren & Drennan, 2008). Nonetheless, the draconian laws are hardly enough to protect the public from identity fraudsters.

LITERATURE REVIEW

The review surveys the problem of identity theft or fraud, which has increased exponentially since the emergence of the internet in mainstream communications, and especially with the rise of online consumer services and shopping. The review surveys the recent development and status of biometrics, with a general preference emerging in the security community for biometrics over existing password or ID card-based security (Gregory, 2008; McCollum, 2005; Mercuri, 2006; Opperman, 2009; Smith & Lias, 2005; Swartz, 2009; Winterdyk & Thompson, 2008). The review then examines the various barriers that as yet stand in the way of broader implementation of biometrics, including economic, systemic and public issues (Dey & Samanta, 2010; Douhou & Magnus, 2009; Kriemer, 2010; Leong & Yerzak, 2004; Palaniappan, 2008; Sullivan, 2009).

Over a decade ago, identity theft was a puzzling and often misunderstood crime. Before 1999, it was estimated that identity theft victimized 40,000 people per year, and imposed a cost on consumers of almost $100 million annually (Saunders & Zucker, 1999). Research suggests that it was in 1998 that identity theft reached a level of critical mass that at last brought a legislative response. The U.S. secret service, which tracked identity theft crimes, found that the dollar value of such crime doubled in the year prior to 1999 and that fraudulent credit reports had climbed from less than 12,000 per year in 1992 to more than 500,000 per year in 1999. As a result, the 1990s were the decade when identity theft or fraud emerged as a crime (Saunders & Zucker, 1999).

While the literature on biometrics evaluation features numerous mathematical demonstrations of new algorithms or methods which will improve a particular type of biometrics, when it comes to use in the real world experts evaluating biometric preferences must also take into consideration the ease of use, perception of usefulness and acceptability of the device as perceived by the public as a leading issue contributing to their practical preferences (Coventry, 2005; Dekking & Hensbergen, 2009; Gorodnichy, 2009; Jain & Pankanti, 2001; Mane & Jadhav, 2009; Schuckers, 2003; Sulovska & Adamek, 2010; Volner & Bores, 2009; Wechsler, 2010). As a result, biometrics in particular, while characterized by highly specialized technical advances in the research, poses evaluation challenges. For this reason, theoretically, iris identification appears to emerge as a researcher preference, but fingerprinting at present remains the most practical and acceptable form of individual biometrics currently available, when taking into consideration costs, ease of use and public acceptability issues (Coventry et al., 2005).

Which biometric system is ultimately most effective remains a robust area of research. At the same time, other researchers are finding that all the so-called unimodal biometrics may

have intractable security gaps that can only be closed by developing a multimodal biometrics model of operation whereby more than one kind of biometric data is taken and analyzed to determine identification, with security breaches greatly diminished by the fact that more than one match is needed in order to confirm identity (Volner & Bores, 2009). The development and testing of multimodal biometric security systems is on the rise, though practical implementation lags behind. At present, experts have their views about individual biometrics, comparing one kind of test with another, but have also begun to evolve toward a new platform of multimodal biometrics, which appear to some to offer the most promising security, to the extent that it may even cause identity theft and fraud to diminish (Gorodnichy, 2009).

With the rise of the internet an identify thief could act through the appropriation of identifying information publicly available in databases on the internet, and thus, technically, without the thief ever obtaining a single identification document not be prosecutable under previous laws. The fact that courts had yet to declare (as of 1999) a person's identity as a tangible personal property, however, limits the relevance of tort law. Invasion of privacy laws also fail to address identity theft as it is concerned with the use of a person's property for commercial advantage. The overall intent of the Deterrence act was "to expressly criminalize identity theft, classify private citizens as direct victims of such conduct, and allow courts to include loss suffered by individual consumers into restitution orders for expenses resulting from rectifying their credit records" (Saunders & Zucker, 1999, p. 189).

Jarillo, Pedrycz and Reformat (2008) estimated that identity theft had resulted in $21 billion lost during 2003. Identity theft was estimated in 2006 to have cost the economy $49 billion per year. At present estimate, identity fraud costs U.S. businesses $53 billion annually (Swartz, 2009) and 3.7% of U.S. adults were victims of identity fraud in 2006 (Goldwasser & Anderson, 2007). Gregory (2008) also noted that by one measure ID fraud cases have risen from 9,000 in 1999 to 77,500 in 2007. Moreover, this number was expected to double in the next five years. Online shopping is one of the engines of this escalation, as a good deal of fraud occurs in online shopping contexts in the form of phishing, in which the fraudster acquires usernames, passwords or credit card numbers (Gregory, 2008). Banks seem to be particularly vulnerable. All of the ways in which banks in particular are working to protect consumers from identity fraud are called cyber armor by some (Goldwasser & Anderson, 2007).

Areas In Which Identity Fraud Emerges

Identity fraud as a crime has emerged in a number of different areas of modern life (Gregory, 2008; McCollum, 2005; Mercuri, 2006; Opperman, 2009; Smith & Lias, 2005; Swartz, 2009; Winterdyk & Thompson, 2008). Identity and document fraud also contribute to what Citizenship and Immigration Canada (2008) termed "irregular migration" of illegals into countries, using stolen documents and false identities. The use of biometric technology to identify people in the refugee, immigration and border facilitation programs of the country is widespread. A field trial of biometric technology was undertaken at visa offices, ports and airports to determine the extent to which biometric devices reduced identity fraud at entry points. The system was then evaluated by a forensic expert in terms of its data accuracy and ability to detect fraud. They found that 97% of the fingerprint and facial biometrics derived from photos were of high quality, that when combined the system matched data 100% of the time and verification was accurate in 96% of the cases. The results also found that both fingerprint and

facial recognition biometric technology were highly accurate and effective in detecting fraud. Some evidence was also provided that "the field trial did deter visa recipients from arriving in Canada through the participating ports of entry," meaning that biometrics served as a deterrent to fraud (Citizenship and Immigration Canada, 2008, p. 19).

Identity also plays a major role in employment, with the law mandating that a person hiring an employee be able to identify them as U.S. citizen based on Social Security card and Permanent Resident ID care. However, document-based identification is highly susceptible to forgery and it is often difficult for employers to know which documents are authentic. This is a particularly pressing problem with regard to the hiring of illegal aliens (Mercer, 2009). To help employers manage the ID verification process the federal government developed E-Verify, which identifies a potential employee by matching data provided by them with a database of social security numbers. The system is able to verify in a few seconds that an employee is eligible to work (Bio-key International, 2010). But the system has been slow to be accepted, with only 12% of new hires checked by it, and also found to be ineffective, failing to reject as ineligible up to 64% of ineligible employees (Elling & Thompson, 2006). Use of the E-Verify system is mandated in only three states, and most employers perceive the system as not easy to use (Bio-key International, 2010). The fact that after using E-Verify employers must then enter the same data to the state labor department website adds to the administrative burden of the system. E-Verify's weak link is that it only matches the presented SSN with the SSN in the system, but does not confirm that the person presenting the SSN is in fact the person in the system, or has stolen a social security card (Bio-key International, 2010).

More disconcerting, E-Verify have validated the Social Security Card as the basis of identification, creating a black market of stolen cards. As one congressman reported, "E-Verify does for identity theft what Prohibition did for Al Capone" (Bio-key International, 2010, p. 6). E-Verify also fail to differentiate between legitimate and fraudulent ID requests if an employer enters the same valid SSN for a number of illegal hires. As a result, any system based on employer document review as the basis of identification is generally considered to be wide open to fraud. Legislators therefore have called for replacing E-Verify with a biometric verification system called BELIEVE, based on the issuance of smart ID cards to all workers, "with a unique biometric template embedded" in it (Bio-key International, 2010, p. 3). In the process, Bio-key International (2010) established a list of key criteria to look out for when evaluating the effectiveness of biometrics, incorporating elements of the Technology Acceptance Model: accuracy, maturity, cost-effectiveness, scalability, ease of use and user acceptance. In reviewing the various biometric possibilities for the system, Bio-key International (2010) concluded that finger-based biometrics is the most mature and cost-effective solution. This is because fingerprinting is accurate, cost-effective, mature (with automatic fingerprint matching going back thirty years), has a high degree of scalability, easy to use and much more acceptable to people than other methods. Bio-key International (2010) also argued that rather than creating a new card system a biometrics check could be added to the existing E-Verify system matching results with a centrally located secure database.

Another source of identity fraud is the theft of employee records from businesses, the SSNs and other elements then used by criminals for fraudulent purposes (Calvasina, Calvasina, & Calvasina, 2007, p. 69). Records theft has been further expedited by laptops, which expedite the process of removing records from company electronic files. By one estimate over 88 million employee records have been compromised in one way or another. As a result, an increased

number of restrictions on the use of a person's SSN have emerged. Companies have also been warned to safeguard records, to limit exposure of records to employees and have also provided identity theft services to employees who have suffered identity theft to instruct them how to respond. That said, while Calvasina et al. (2007) argued that "a top down approach with genuine commitment of resources to effectively protect employee personnel information is necessary" (p. 78), it may be that document-based security as a paradigm is outdated.

Types of biometrics: face recognition.

One of the most promising developments in biometric system fraud prevention is face recognition technology. Face recognition has been applied to personal identification, security applications and law enforcement (Bhattacharyya, Ranjan, Alisherov, & Choi, 2009). One of the major benefits of face recognition is that it is less intrusive than other biometric systems such as fingerprinting.

Eigenfaces, Line Edge Maps, Fisherfaces, and other methods have also been developed for facial recognition. Jarillo et al. (2008) argued that the best elements of all of these methods should be synthesized to create the optimal facial recognition system, with enhanced global accuracy overall.

Palm scanning.

Theft of medical records for use in health insurance fraud is yet another dimension of the identity theft problem. To prevent this, hospitals have begun to adapt biometric security to add an extra layer of security to records. Kriemer (2010) reported on the decision by the Hospital to implement palm scanning. The leadership decided on palm scanning over other biometrics because the patterns of veins in one's hands is unique in each person, and even identical twins do not have identical vein prints. To forestall public worries about germs, or resolution degradation due to print residue, newer palm scanners do not require contact with the scanner

Voice biometrics.

Biometrics is also being deployed on the Internet, mainly through voice biometrics. Besacier, Mayorga, Bonastre, Fredouille and Meignier (2003) noted that introducing biometrics involves a multidisciplinary task involving person authentication techniques based on signal processing, statistical modeling and mathematical fusion methods, not to mention data communications and online data security. Besacier et al. (2003) noted that while promising, voice recognition on the internet presents technicians with a number of problems including transcoding modification, transmission errors, time response and the fact that resulting speech packets could still be intercepted by impostors.

Iris biometrics.

Iris-based biometric authentication is becoming more popular, as it has been found that the iris results in the most accurate and reliable measure of identity, because of the rich texture of iris patterns, the inimitable quality of irises and because they remain the same for a lifetime

(Podio & Dunn, n.d.). Iris features alone identified in research include freckles, corneas, stripes, furrows and crypts. Because of the specificity of iris features it is also more likely that matching it to the template image already in the database will be more accurate (Huber, Stogner, & Uhl, n.d.). A science has emerged with phase-based methods, zero-crossing representation and texture analysis contending as the primary means to extract and match iris feature data. Matching techniques which match the data to the template are also varied, including the Hamming distance, Weighted Euclidean distance and Normalized correlation measurement techniques (Wayman, Jain, Maltoni, & Maio, 2005). Thus, there are a number of available criteria to evaluate the potential effectiveness of iris recognition for combating identity fraud. But iris authentication remains constrained by the fact that it involves complex processes and is very expensive to compute.

Exotic forms of biometrics.

Another type of biometric authentication involves recording personal behavior such as keystroke dynamics while typing in information in a system. The question is whether or not keystroke dynamics as a form of biometrics are reliable enough as a security instrument to be useful in combating identity fraud (Monrose, & Rubin, 1999). Keystroke dynamic analysis studies such factors as dwell times, or how long a key is held pressed, and flight times, or the time between consecutive press times. It originated as a discipline during the Second World War when decoders found that every individual delivering Morse code spaced and stretched out dots and dashes using a unique rhythm, termed the operator's fist (Douhou & Magnus, 2009). By identifying the fists of various German radio signalers around Europe, British agents were able to determine where the German army was moving. Statistical and data mining ways to extract "fists" from keystroke dynamics data has advanced the field. Some keystroke dynamics theorists argue that one can distinguish between real users and hackers by their keystroke characteristics (Douhou & Magnus, 2009).

In an experimental test of 1254 participants at the University of Amsterdam designed to test keystroke dynamics reliability, Douhou and Magnus (2009) found that keystroke dynamics can be a reliable security instrument for authentication, but can only be so if used with other instruments. Also, dwell times were found to be more discriminatory and powerful than flight times in identifying users but keystroke dynamics is more useful for authentication/verification.

Palaniappan (2008) proposed a biometric method for verification of identities making use of brain waves recorded on an electroencephalogram while the user is asked to perform some simple thought activities. All persons have brainwaves patterns that are unique, making brain waves yet another source of biometric measurement. A two-stage authentication method was developed and tested. The model placed values on EEG features through autoregressive coefficients, channel spectral powers, inter-hemispheric channel special power differences and channel linear and non-linear complexity values. These were measured as subjects were asked to think of nothing in particular to establish a baseline, do a math activity, a geometric figure rotation activity, a letter composing activity and a visual counting activity. A test found that the EEG perfectly identified individual subjects, strongly suggesting that EEG features derived from thought activities are a potential biometric that is "highly resistant to fraud" (Palaniappan, 2008, p. 59).

METHODOLOGY

The purpose of this qualitative study was to ascertain the perceptions of biometric-industry experts on whether or not biometric modalities will combat identity fraud. This study employed a qualitative phenomenological research design and interviewed biometric industry experts from various geographical locations in the United States. The data are in form of participant responses to semi-structured interview questions. The responses were recorded and transcribed to capture the lived experiences of the 10 selected biometric-industry experts from various geographic locations in the United States. The data were then coded based on the Leeds attributional coding system and analyzed based on the modified van Kaam (1959) method.

The participants were identified through the following group, the LinkedIn.com group called IEEE Certified Biometrics Professional (CBP) group. The participants were evaluated according to their expertise in the topic of the study (Cassell & Symon, 2004). The assessments were based upon the potential for the research participant to provide valuable information on the concept of biometrics because of their professional experience in this field. The lived experience is based on their level of education and the number of years experience working in the biometric industry, either as researchers, developers, or security analysts (Marshall & Rossman, 1999).

This study is the first academic researches to probe the perceptions of biometric experts on whether or not biometric modalities will combat identity fraud. The research questions that guided this study were designed to investigate the perceptions of biometric experts on whether or not biometric modalities will combat identity fraud. The following questions served to guide the study:

Research Questions

1. In what ways are biometric modalities effective in combating identity fraud?
2. What are hindrances to the effectiveness of biometric modalities in combating identity fraud?
3. Which biometric modalities do biometric experts perceive to be most effective in combating identity fraud?

RESULTS

The study's objective was to identify factors relevant to Research Questions 1-3 as reflected in the interview data. Each interview was viewed as a single incident. That is, each interview was considered individually in the analysis. Common themes were identified across the data with regard to addressing the research questions.

Results for Research Question 1

Research Question 1 was *in what ways are biometric modalities effective in combating identity fraud?* The four primary themes related to this research question are summarized in this section. This section includes tables summarizing the definition of the identified themes, the frequency of occurrence for the themes and subthemes, as well as the number of interviewees that mentioned a specific theme and subtheme. As reflected in Table 1, the primary themes were

physical traits, better identity protection, biometrics should be combined, and biometrics are reliable.

Table 1. Themes and Definitions for Research Question 1

Themes and Subthemes	Definition
Physical traits	Physical traits of biometrics are most useful
Better identity protection	Biometrics provides better identity protection than other technologies.
Biometrics should be combined	Biometrics are effective when combined with other modalities
Biometrics are reliable	Biometrics are reliable and not easily forgotten, lost, falsified or stolen etc.

Table 2 shows the frequency with which the themes appeared across interviews and across the data.

Table 2. Frequency of Themes for Research Question 1

Themes and Subthemes	Number of interviewees mentioning this theme	Total exemplar quotes
Better identity protection	7	8
Biometrics should be combined	4	7
Biometrics are reliable	5	6
Physical traits	1	1

Better Identity Protection

The most frequently occurring theme for Research Question 1 was *better identity protection*. This theme was defined as Biometrics provides better identity protection than other technologies and was mentioned eight times in seven interviews. According to Participant A, "Any of the physical trait biometrics I think would be most useful in combating identity fraud. And I say physical traits because I think that it really boils down to user acceptance of providing biometrics". Participant B furthered this sentiment by stating,

> In combating identity fraud, biometrics can be very effective in combating identity fraud provided that there is a trusted enrollment of an individual into the biometric system. What I mean by that is that you need to --if you are able to make sure when a person enrolls in the biometric system that he or she is who they claim they are, then biometric can --biometrics can probably provide better identity protection than any other known technology.

Similarly, Participant C stated, "Biometric modalities absolutely will be useful in combating identity fraud". Later in the interview he elaborated:

> Biometric information is part of a person. Since biometrics is intimately tied to a person, they are considered to be more reliable and not easily forgotten, lost, stolen, falsified, or guessed. A biometric identifier relies on unique biological information about a person.

Participant G shared, “Biometric modalities absolutely will be useful in combating identity fraud”. Participant D indicated “Given the uniqueness of biometric technology, the use of any biometric modality in concert with other access control strategies can provide an effective means to thwart identity fraud”. Participant E indicated Biometrics are “Useful in the sense that if there were an infrastructure or actually several infrastructures in place to solve several fairly well understood problems, then iris or fingerprints could eliminate identity fraud”. In the final exemplar quote, Participant I stated, “Biometric modality will be very useful in combating identity fraud because of the difficulties in obtaining unique biological characteristics of an individual”.

Biometrics Should be Combined

The next theme for Research Question 1 was *Biometrics should be combined*, which refers to Biometrics being effective when combined with other modalities. This theme was mentioned seven times in four interviews. Several interviewees felt that the most effective biometrics were those that could be combined to maximize protection. Participant C shared,

> Physical access controls are one way to prevent identity fraud. However, in a security environment, it is best practice to combine physical access controls with logical authentication types. In order to provide a higher level of security, it is more effective to authenticate users based on a mix of authentication types: Biometrics and logical.

He further elaborated on this issue:

> Biometric technologies can be combined to provide enhanced security. The combined use of two or more biometric technologies in one application is called a multimodal biometric system. Instead of relying on only one technology, a multi-modal system combines several biometric technologies to increase the likelihood of finding a match will be increasingly feasible as hardware and system cost decreases to more acceptable level. A multimodal system creates an even greater level of assurance of an accurate match in verification and identification systems.

Participant H shared a similar sentiment with regard to maximal protection via combining biometrics:

> Given the uniqueness of biometric technology, the use of any biometric modality in concert with other access control strategies can provide an effective means to thwart identity fraud. More specifically, using a defense in depth approach increases the level of complexity, limiting the attack surface which could lead to unauthorized access.

Participant J stated, “Absolutely, biometric modalities will be useful in combating identity fraud especially when combined with other form of authentication types”.

Participant F provided a detailed response with regard to why the combining of Biometrics is best. He explained,

> So one of the things is that biometrics are not secrets. Often in combating identity fraud, the use of secret is a very important thing, all right, so whether that be your pin or password or it be your mother’s maiden name or it be a cryptographic key, those things are very important in terms of online security. So, for the most part, biometrics is best used and probably most successful as something that’s used in combination with other authentication factors. The standard factors being something you had, something you know, and something you are.

He then further stated, “Its best used in combination with the other ones. So that’s just a general statement about the use of biometrics and how to be successful independent of the particular application that’s involved”.

Biometrics Are Reliable

Another common theme for Research Question 1 was *Biometrics are reliable*, which refers to Biometrics being reliable and not easily forgotten, lost, falsified or stolen. This theme was mentioned six times in five interviews.

Several interviewees explicitly mentioned the reliability of Biometrics. For example Participant C said “Since biometrics is intimately tied to a person, they are considered to be more reliable and not easily forgotten, lost, stolen, falsified, or guessed”. Participant G indicated “Because it’s about physical characteristics so they are considered to be more reliable and not easily forgotten, lost, stolen, falsified, or guessed”. Participant E explained why Biometrics are so reliable. He indicated “People very seldom forget to bring their irises or their fingers to work or any other parts of their body, so biometrics is highly compelling for convenience”. Later he also mentioned that “it’s phenomenal and if you do go with convenience, then you can also use the biometric to prevent identity fraud”.

Participant D also highlighted the reliability of specific biometrics by stating Biometrics are, “Very effective. Biometrics is robust authentication methods in addition to token or passcode”.

Participant F provided a detailed example and explanation for why Biometrics are reliable. He shared the following:

> Because, as an example, if I were to do it myself and say this fingerprint belongs to me, Participant F, how do you know that? So, if you allow - - if something is self-asserted, then there’s very little level of trust and therefore very little use in terms of combating fraud. So one of the most important things in the entire process is this idea around what’s referred to as registration, so at the actual creation of the biometric and its binding of the identity in the identity registration process that you use things which do a strong cryptographic binding as well as a process which includes a separation of roles in terms of the authorization of the binding between the credential and the individual.

Physical Traits

The next theme for Research Question 1 was *physical traits*, which refers to the physical traits of biometrics are most useful. This theme was mentioned one time in one interview. Job rotation was a common practice. In a single quote, Participant A stated, “Any of the physical trait biometrics I think would be most useful in combating identity fraud. And I say physical traits because I think that it really boils down to user acceptance of providing biometrics”.

Results for Research Question 2

Research Question 2 was *what are hindrances to the effectiveness of biometric modalities in combating identity fraud?* The five primary themes related to this research question are summarized in this section. This section includes tables summarizing the definition of the

identified themes, the frequency of occurrence for the themes and subthemes, as well as the number of interviewees that mentioned a specific theme and subtheme. As reflected in Table 3, the primary themes were difficulty with implementation, difficulty with utilization, difficulty accepting biometrics, and lack of tailoring.

Table 3. Themes and Definitions for Research Question 2

Themes	Definition
Difficulty with implementation	Difficulty with implementing biometrics
Cost	Costs for implementation of Biometrics can be high
Training	Lack of training for using Biometrics
Infrastructure	Lack of infrastructure for implementing Biometrics
Difficulty with utilization	Difficulty for users to "use" biometrics
Matching rate	There can be matching rate problems with Biometrics
Fake enrollments/security flaws	Fraudulent identities can be enrolled in a Biometric system.
Operational errors	Operational errors as a difficulty of Biometric utilization
Difficulty "accepting" biometrics	Difficult for users to accept providing Biometrics
Difficulty providing biometrics	"Ease of use", difficulty for users to provide biometrics
Negative connotations	Users' negative connotations about biometrics (e.g., finger printing for criminals).
Lack of trust	Lack of trust among users
Lack of tailoring	Biometrics should be tailored to the specific threat and context.
Lack of collaboration	Lack of collaboration between industry and government

Table 4 shows the frequency with which the themes appeared across interviews and across the data.

Table 4. Frequency of Themes for Research Question 2

Themes	Number of interviewees mentioning this theme	Total exemplar quotes
Difficulty with implementation		
Cost	8	9
Training	1	2
Infrastructure	1	2
Difficulty with utilization		
Matching rate	2	3
Fake enrollments/security flaws	1	1
Operational errors	1	1
Difficulty "accepting" biometrics	3	6
Lack of trust	7	8
Difficulty providing biometrics	3	3
Negative connotations	1	2
Lack of collaboration	4	4
Lack of tailoring	2	4

Difficulty with Implementation

The most frequently occurring theme for Research Question 2 was *difficulty with implementation*, which refers to difficulty implementing biometrics. Difficulty with implementation was further categorized into three subthemes: (a) *cost*, (b) *training*, and (c) *infrastructure*. Each subtheme is discussed below.

Cost. The subtheme *cost* refers to costs for implementation being high. It was mentioned nine times in eight interviews. Participant A stated that cost is associated with implementation: "matching, has to be low cost enough that it would start allowing the systems to become ubiquitous. If the systems are easily integrated into be it purchases systems or what have you, then you can expect a high level of adoption on the retail side". Similarly, Participant B shared the following:

> Roadblocks are primarily the cost of biometric system management. It's not just the cost of biometric devices, which are actually fairly inexpensive, but the cost of management of a system in which you have trusted enrollment of the individual, in which you have maintenance of a secure biometric database, and you have proper privacy and recourse rights for the users who want to be removed from the system or who want to make sure that biometric database would not further compromise their identity. So the roadblocks are mostly the cost of implementation.

When Participant C was asked about potential roadblocks for Biometrics he simply stated, "Cost of hardware". Participant G also indicated "cost of hardware".

Several interviewees mentioned specific costs associated with Biometrics. For example, Participant D said I, "would I need to purchase additional technology etc. in order to effectively use this service". Participant E mentioned the cost of iris and DNA Biometrics:

Iris, by its very nature, lends itself to liveness detection, but there is no equipment at an affordable price, nor is it in place. DNA, it takes too long and it's far too expensive, so that's not going to be a factor.

Participant E further explained the nature of these costs is associated with lost passwords:

> They write them down, they lose many of them, they reuse the same ones, which is risky, but because of the different conventions for passwords, they end up with large number of passwords anyway which have to change fairly frequently, so people regularly find themselves shut out of sites. Password resets are extremely expensive. 40% of helpdesk costs nationally are for password resets, typically after long weekends or after people return from vacations. So there's a real issue here of convenience and cost.

Richard indicated cost was one of several roadblocks to Biometric implementation including, "cost of hardware". Whereas Participant I mentioned "Some possible road blocks may be the cost of the equipment".

Training. The subtheme *training* refers to lack of training in how to use biometrics as a difficulty for implementation of Biometrics. It was mentioned two times in one interview. More specifically, Participant I said, "Some possible road blocks may be ….. Training required to properly implementing the technology". He also mentioned that additional training would be required for users, "Also awareness training required for users"

Infrastructure. The subtheme *infrastructure* refers to the lack of infrastructure for implementing Biometrics as a difficulty for implementation of Biometric. It was mentioned two times in one interview. Participant E indicated, "there is no infrastructure in place, at an economically affordable—well, there's no infrastructure in place period and at the moment, it's not economically affordable to use biometrics to verify your identity". He further explained the nature and importance of such an infrastructure:

> Photo face matching has come a very long way, but for really large numbers of people it's not remotely reliable enough for this purpose, nor is there a ready way to do liveness detection over the internet when it's an unattended situation so there's that, and then I think the last major piece is there's no identity broker service in place. Even if we had a mechanism to prove that you're you and to give you a token or some kind of a documentation or a digital identity online and even if we had solved the problem of collecting your biometrics and proving liveness, there is no centralized place that a merchant or another person that wants to verify your identity can go to get that information back.

Difficulty with Utilization

The next theme for Research Question 2 was *difficulty with utilization*, which is defined as users' difficulty with using biometrics. Difficulty with utilization was further categorized into three subthemes: (a) *matching rate*, (b) *fake enrollment/security flaws*, and (c) *operational errors*. Each subtheme is discussed below.

Matching rate. The subtheme *matching rate* refers to the mention of matching rate problems with biometrics. It was mentioned three times in two interviews. Participant A explained the nature of matching rate errors in detail:

> For example, a false match rate might allow somebody on a military base who's not supposed to be. A false non-match might let a known bad guy get away from law

> enforcement. Other commercial entities, such as Disney World, do use biometrics but their thresholds are rather low because they would rather have somebody who let's say hasn't paid for a ticket enter the system because the cost of one additional person is rather low versus letting a legitimate user be turned away. This model does not transfer into healthcare and into finance to industries that have a great potential for use - - for biometrics. Having somebody else enter your bank account is absolutely not acceptable nor is having somebody who isn't allowed to review your medical records suddenly gain access. So, people do not like the probabilistic nature of biometrics even though this is the same type of decision process that's used in many other circumstances. I think that the overall matching rates need to be improved under a host of environmental conditions, so non-laboratory meaning that there are accommodations for spoofing methods, accommodations for variances in light, presentation, et cetera. And then you will finally start seeing biometrics starting to become more ubiquitous.

Participant F mentioned problems with matching rates by mentioning, "And then in addition to those things, the performance, both related to enrollment and recognition rates, varies among biometric technologies. And so those always need to be things that are taken into consideration. He went on to explain,

> But of course in the case of putting your hand down on the platen, some people have problems in rolling their fingerprint and the recognition rate on fingerprints aren't as high as they are on iris, so there are these tradeoffs around registration and recognitions and false positives and false rejects that you always have to take into account.

Fake enrollment/security flaws. The subtheme *fake enrollment/security flaws* refer to the ability for fraudulent identities to be enrolled in a biometric system. It was mentioned one time in one interview. In the only exemplar quote for this subtheme, Participant B stated, "But if a fraudulent identity is enrolled into the biometric system, then the biometric system is as ineffective as any other technology". There were no other exemplar quotes for this subtheme.

Operational errors. The subtheme *operational errors* refer to operational errors as a difficulty of Biometric utilization. It was mentioned one time in one interview. When asked about Roadblock to Biometrics, Participant D answered, "Quality of biometrics and operational error. Most of the data collect is via soldiers with little training and even when they are trained, they get rotated out of that job".

Difficulty Accepting Biometrics

Difficulty accepting Biometrics was another common theme for Research Question 2. The exemplar quotes were further classified into three subthemes: (a) *lack of trust*, (b) *difficulty providing biometrics*, and (c) *negative connotations*.

Lack of trust. The subtheme *lack of trust* refers to lack of training in how to use biometrics as a difficulty for implementation of Biometrics. It was mentioned eight times in seven interviews. Participant A highlighted the importance of gaining users' trust that their privacy would be protected when using Biometrics. He shared:

> I think that privacy will - - in order to promote privacy, you'll have individuals be willing to provide biometrics if they can properly understand, in very simplistic terms, how their biometrics will be captured, where they will be stored, and what control users have over the biometrics once submitted, especially in ways to prevent biometrics from being

> distributed to other service providers and to have the users revoke the biometrics if they feel that they need to do so.

He then further explained:

> The first one is obviously the rest of your investigations point of privacy remains a big concern and this is not necessarily a purely technological implementation. Privacy is far more about culture, it's about legal issues, and it is not something that technology alone can resolve. Certainly there has to be policy and process in place to define what privacy is and this will definitely change per demographic and how it should be implemented.

Participant C and Participant G highlighted the issue of trust as well. Participant C mentioned that trust is an "an issue of privacy and confidentiality". Participant G shared, "As far as road blocks I would have to say privacy, user's acceptance of the system". Participant D also mentioned users' lack of trust and stated users ask "and how secure in my information upon process and storage?" Participant E mentioned that stakeholders are not trusting with regard to how their Biometrics will be used, "plus there is some concern in the civil liberties community as well as among the public about making their biometrics available". In a final exemplar quote, Participant I said that trust in privacy would be an issue, "privacy perceptions associated with certain biometric modalities such as fingerprinting" are related to trust.

Difficulty providing biometrics

The subtheme *difficulty providing biometrics* refers to "ease of use" problems and difficulty for users to provide Biometrics. This subtheme was mentioned three times in three interviews**.** Participant D stated ease of use is a barrier, "First, ease of use, i.e. will I be accepted or rejected even though I provide the right information to authenticate". Participant J said barriers to the use of Biometrics are multifaceted and include issues with "ease of use". Participant F mentioned,

> And so the ability for biometrics to be used in combating identity fraud are very much related to their ease of use, and their ease of use is a fact that they can be applied in or to a majority of your identity transactions. So until the terminalization problem is solved, then it becomes difficult.

Negative connotations

The subtheme *negative connotations* refer to users' negative connotations about Biometrics (e.g., finger printing for criminals). This theme was mentioned two times in one interview. Participant A explained the negative connotations associated with Biometrics:

> Other modalities, which are still under research, may not be able to accomplish this or may be more difficult for users to implement, such as DNA. DNA would be extremely useful but not very practical for most applications. Individuals also associate fingerprinting with criminal activity and there is a biased against using them, although this is the one biometric that most people are familiar with.

He further explained, "These systems have been shown to have high accuracy rates once a user has been hebetated to using them and users are more likely to accept this form of biometrics because it doesn't have negative connotations".

Lack of Collaboration.

The next theme for Research Question 2 was *lack of collaboration*, which refers to the lack of collaboration between industry and government to enhance the effectiveness of biometric modalities. This theme was mentioned four times in four interviews.

Participant C was explicit about the lack of and need for collaboration. He said, "Another road block will be lack of consistent collaborations between commercial industries and government". Participant G also said, "Another road block will be lack of consistent collaborations between commercial industries and government". Participant E explained how stakeholders could collaborate given their shared situation:

> The banks and other financial institutions have mechanisms in place that make the losses acceptable to them. The banks that are interested in addressing biometrics are primarily doing it as one more thing to enhance the customer relationship, not to save money. The government is deferring to the private sector and there's just no clamor going on in the private sector.

Similarly, Richard indicated, "Fingerprint has the most potential to combat identity fraud because the infrastructure is already in existence. But government and industry stakeholder, like banking and healthcare have to collaborate".

Lack of Tailoring

The next theme for Research Question 2 was *lack of tailoring*, which refers to the lack of tailored Biometrics to meet specific threats and contexts. This theme was mentioned four times in two interviews. Participant B stated,

> It's very difficult to say biometrics is going to be equally effective for each of those specific types of identity theft methods, but in some of them, for example, they could be better suited to provide protection than in the others.

He went on to explain,

> For example, in the level of detail that someone will have about my behaviors from the two types of theft are significantly different and therefore if you have one document about me, then biometrics may be sufficient. If you have my ten-year history of all the payments and everything and you know who the people I work with are, you can then get the information, other information from Facebook and stuff like that about me. You can get my photos. You can get all the other things. Whether biometrics per se can guard against that, that's more questionable. So that's where I think the level of detail in designing and understanding the use cases for protection would be very helpful.

In the other exemplar for this theme, Participant C explained:

> No single biometric can meet the requirements of all applications. Thus, no biometric is optimal. The match between a specific biometric and an application is determined by the operational mode of the application and the properties of the biometric characteristic. Different applications and environments encounter different constraints.

He furthered his point by stating, "The effectiveness of a biometric system relies on how and where it is used. Before implementing a system, evaluate the strengths and weaknesses of each biometric modality relative to its application".

RESULTS FOR RESEARCH QUESTION 3

Research Question 3 was *which biometric modalities do biometric experts perceive to be most effective in combating identity fraud?* The four primary themes related to this research question are summarized in this section. This section includes tables summarizing the definition of the identified themes and subthemes, the frequency of occurrence for the themes and subthemes, and the number of interviewees that mentioned a specific theme and subthemes. As reflected in Table 5, the primary themes were facial matching, Biometrics acceptable to users, retina scans, and combined biometrics.

Table 5. Themes and Definitions for Research Question 3

Themes	Definition
Facial matching	Facial matching is most effective
Facial matching: ease of implementation	Facial matching is easy to implement and integrate
Facial matching: user acceptance	Users are more likely to accept facial matching
Biometrics acceptable to users	Biometrics that are acceptable and comfortable to users are the most effective
Retina Scans	Retina scans are most effective
Combined biometrics	A combination of biometrics is most effective.

Table 6 shows the frequency with which the themes appeared across interviews and across the data.

Table 6. Frequency of Themes for Research Question 3

Themes	Number of interviewees mentioning this theme	Total exemplar quotes
Combined biometrics	5	8
Facial matching	4	4
Facial matching: ease of implementation	1	1
Facial matching: user acceptance	3	3
Biometrics acceptable to users	1	1
Retina scans	1	1

Combined Biometrics

The most frequently mention theme for Research Question 3 was *combined Biometrics*, which is defined as reference to the idea that a combination of biometrics is most effective. This theme was mentioned eight times in five interviews. Participant H's statement that combining several biometrics is ideal is an example of this theme. He recommended a "Fusion of iris, fingerprint and face recognition – for fast identification". Participant E recommended "friction ridges and also iris, and the reason that I feel so is they have resolving power". He later explained why he made this recommendation by sharing "But friction ridges, typically fingerprints, are highly individualizing and comparatively inexpensive and quick to capture, same thing with iris". Participant J felt the same and mentioned, "The modalities I feel most effective in combating identity fraud would be fingerprint, face matching, and iris". Participant I's response was detailed:

> I feel that since there are advantages and disadvantages of implementing each of the biometric modalities, it will be beneficial to use a combination of modalities to increase the difficulties of performing identity fraud by requiring multiple biological characteristics. This will also help reduce false acceptance rate (FAR) that may occur if only one biometric modality is used. The system can cross reference biological characteristic information obtained from other biometric modalities to confirm the user's identity and not rely on one single biometric modality.

Participant F recommended a combination of Biometrics be used, as indicated by his previously mentioned quote for Research Question 1.

Facial Matching

The next theme for Research Question 3 was *facial matching*, which refers to feeling that facial matching is most effective. This theme was mentioned four times in four interviews. Participant A explained:

> Well, I believe that the most effective would be facial matching. And the reason why I pick on face is that it - - when you capture a face, you are also at the same time, potentially, capturing many other biometric modalities as a subgroup. Obviously the first one that comes to mind is iris; however, there have been studies on ear biometrics, there have been studies on lip biometrics, and other types of facial topology features.

Participant B shared:

> I feel that modalities that will be most effective will be those that the users feel the most comfortable using without any special hardware, so I feel that face recognition and - - face recognition probably would be the most effective ones because users will accept it easier than fingerprint recognition or iris recognition.

Participant C also mentioned, “The modalities I feel most effective in combating identity fraud would be face matching”. Participant G also shared, “The modalities I feel most effective in combating identity fraud would be face matching”.

Other exemplar quotes for this theme were further classified into two subthemes: (a) *facial matching: User acceptance* and (b) *facial matching: ease of implementation.*

Facial matching: User acceptance

This subtheme refers to the idea that users are more likely to accept facial matching. It was mentioned three times in three interviews. Participant B explained that he though users would find facial matching more acceptable:

> I feel that modalities that will be most effective will be those that the users feel the most comfortable using without any special hardware, so I feel that face recognition and - - face recognition probably would be the most effective ones because users will accept it easier than fingerprint recognition or iris recognition.

Participant C echoed these sentiments by saying, “face matching, because it’s not invasive. Many people are use to it and accepting of it”. In a final quote, Participant G indicated “face matching; it is less invasive and somewhat acceptable to the general public”.

Facial matching: Ease of implementation

This subtheme refers to the idea that facial matching is easy to implement and integrate. It was mentioned one time in one interview. Participant A stated,

> So I think having face understood and implemented would probably be the easiest one to integrate. Most people are very familiar with - - and find it a very acceptable to smile for a camera and already their identity credentials have some type of facial picture incorporated.

Biometrics Acceptable to Users

The next theme for Research Question 3 was *Biometrics acceptable to users*, which is defined as the idea that Biometrics that are acceptable and comfortable to users are the most effective. This theme was mentioned one time in one interview. As previously mentioned, Participant B indicated, "I feel that modalities that will be most effective will be those that the users feel the most comfortable using without any special hardware".

Retina Scans

The final theme for Research Question 3 was *retina scans,* which refers to the idea that retina scans are most effective. This theme was mentioned one time in one interview. In the only quote indicative of this theme, Participant D shared:

> I believe that Retina scan offers the most effective safeguard in combating identify fraud. Reason being, it looks as the blood vessels in back of a person's eye that is unique to an individual. It is so complex and effective that studies have shown that even identical twins do not share a similar pattern

RESEARCH QUESTIONS ANSWERED

Conclusion from Research Question 1

Qualitatively, the findings and interpretation of data and interview responses echoed the following conclusion: 70% of the experts interviewed agreed that biometric modalities offer better identity protection; 50% of experts interviewed agreed that biometrics are reliable to effectively combat identity fraud; 40% of experts interviewed agreed that biometric modalities should be combined to maximize its effectiveness in combating identity fraud. Only one of expert contended that any physical trait biometric is sufficient to effectively combat identity fraud.

Based on the expressed expert opinions, the conclusion is that biometric modalities will be effective in combating identity fraud. This conclusion mirrors the body of literature reviewed in and the outcome of the qualitative component of this study. This conclusion has answered the Research Question 1.

Conclusion from Research Question 2

The experts contended that the threshold for both FAR and FRR should be normalized or improved under a host of environmental conditions, even to the point of accommodating, for instance, spoofing methods and variances in light. Another expert expressed that the negative connotations of certain biometric traits are hindrances. For example, the expert believed that fingerprinting and DNA are associated with criminal activity and users are likely to feel such modalities are inherently biased. Also, operational errors and training are often roadblocks or hindrances to the effectiveness of biometric modalities in combating identity fraud, according to 20% of the experts interviewed for this study.

The conclusion is that there are numerous barriers to the effectiveness of biometric modalities in combating identity fraud. This conclusion far surpasses the already-established knowledge and information reported in the body of literature reviewed. This conclusion has answered the Research Question 2.

Conclusion from Research Question 3

The conclusion is that facial matching will be the most effective biometric modality in combating identity fraud. Even though this conclusion contrasts with Li and Wechsler's (2009) assertion in the literatures reviewed that face recognition biometrics are not good at avoiding occlusion or disguise that is intentional or caused by environment noise, this conclusion has answered the Research Question 3.

The results and responses of the experts' opinions in this study validated the concept that biometric modalities will combat identity fraud. Based on the result of this qualitative study, this researcher underscores the expressed opinions of the interviewed biometric experts that biometric modalities will combat identity theft. The findings of this study revealed that biometric modalities will help government entities, banking institutions, healthcare providers, travel and tourism institutions, and individuals combat identity fraud. In the next section, the author discusses limitations of the study.

DISCUSSION

A driving force promoting the use of biometrics for security today is protection against identity fraud. Biometrics suffers from perception problems; however, a majority of the general public views biometrics as secret, even though biometrics are simply exceptional physiological identifiers. Some biometric characteristics can still be easily stolen or compromised (Mark, Debjani, Vijay, & Ernst, 2008), for example, "a fingerprint can be acquired from objects touched by the person; iris data can be obtained from the person's image captured by a camcorder" (p. 3965).

One of the most significant challenges to the use of biometrics is the potential permanence of a breach. If a biometric feature is compromised due to theft, such a loss may be permanent. Passwords and credit cards, if stolen, can be reissued or changed, which reduces the threat of theft. The question remains, what solution would preclude a fraudster from accessing files that contain the binary property of a biometric feature (Mark et al., 2008).

This study reveals an important salient challenge. Biometrics fails to provide alternatives to *failure to enroll*, which identifies people who can never use the system, and the *failure to acquire* rate, or the number of users unable to generate an image when using a device (Coventry, 2005). Consequently, a good biometric system needs a fallback strategy that allows these users to gain another way into the system. These challenges then must be factored into an evaluation of any biometric technology before procurement and or deployment.

Nevertheless, the perception of biometric technologies, its capability to combat identity fraud, and the convenience of preserving privacy are progressively becoming more significant to governments, businesses, as well as individuals. These developments are the drivers for adoption and implementation of biometric technologies to combat identity fraud. Furthermore, the ability to identify individuals almost to the degree of certainty is one of the biggest advantages of biometric technology. For example, biometric ability to identify individuals is being used on a daily basis by police officials for investigation.

CONCLUSION

Biometrics is becoming essential for dependable and unattended human-identification systems. Even though some biometric issues still warrant resolutions, the applicability of biometric modalities in government, public and private sectors is imminent and will intensify in the near future. Although biometric technologies are not foolproof, they are far superior to userids and passwords in averting compromise of sensitive information or data. Furthermore, several shortcomings of biometric systems can be overcome by multimodal biometrics, which appear to offer the most promising security, even to the extent that they may even cause identity fraud to diminish (Gorodnichy, 2009). Additionally, the use of any or multi-biometric modalities in the future may assist in thwarting catastrophic nationwide disasters such as 9/11, and prevent innocent individuals from becoming victims of identity fraud because of deficient identification procedural systems.

Finally, this study, through expert opinion, has provided data on how biometric identification can add an important layer of defense to identifying a person. In the future, government, corporations, and technology adopters may be interested in the data collected for the purpose of this research, especially when considering the adoption of biometric modalities to help combat identity fraud.

RECOMMENDATION FOR FUTURE RESEARCH

This study focused on perceptions of biometric experts about whether or not biometric modalities will combat identity fraud. A starting point for subsequent studies could be working to understand the perceptions of government biometric policymakers. A focus for such research could entail why biometric technologies, with all its promise, have not been wholeheartedly adopted across all government agencies. Another potential area for future research is to investigate whether biometrics is accepted more in particular arenas, such as banking, education, military, etc. Such a study may help gain additional clarity on the acceptance of biometrics.

REFERENCES:

Aguilar, K. (2009). Keeping one's personality and humanity in the electronic and cyber age. *UST Law Review*, *54*, 81-120.

Besacier, L., Mayorga, P., Bonastre, J. F., Fredouille, C., & Meignier, S. (2003). Overview of compression and packet loss effects in speech biometrics. *IEE Proceedings Online, 150,* 372–378. doi:10.1049/ip-vis:20031033

Bhattacharyya, D., Ranjan, R., Alisherov, F. A., & Choi, M. (2009). Biometric authentication: A review. *International Journal of u- and e- Service, Science and Technology*, *2*(3), 13--28.

Bio-key International. (2010). *Reducing illegal employment through the use of biometrics: Options and recommendations.* Retrieved from http://www.bio-key.com/everify-12-10.pdf

Bochkov, Y., Chiem, J., & Sai, Y. (2007, April 15). *Use biometric techniques in combating identity theft.* Los Angeles, CA: Loyola Marymount University. Retrieved from http://academic-papers.org/ocs2/session/Papers/D7/843.doc

Burton, D., & Davis, J. (2002, July 22). Identity theft has become a new threat to national security. *Insight on the News*. Retrieved from http://findarticles.com/p/articles/mi_m1571/is_26_18/ai_90041153/

Calvasina, G. E., Calvasina, R. V. & Calvasina, E. J. (2007). Preventing employee identity fraud: Policy and practice issues for employers. *Journal of Legal, Ethical and Regulatory Issues, 10,* 69–80.

Citizenship and Immigration Canada. (2008). *Biometrics planning project: Biometrics field trial.* Retrieved from http://www.cic.gc.ca/english/pdf/pub/biometrics-trial.pdf

Clarke, E. (2009), How secure is your client data? 5 questions you should ask your IT professionals. *Journal of Financial Planning*, Jan/Feb, 24–25.

Cassell, C., & Symon, G. (2004). *Essential guide to qualitative methods in organizational research*. London, England: Sage.

Coventry, L. (2005). Usable biometrics. Retrieved from http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/ch10-1coventry.pdf

Dekking, M., & Hensbergen, A. (2009). A problem with the assessment of an Iris identification system. *Society for Industrial and Applied Mathematics Review, 51,* 417–422.

Dey, S., & Samanta, D. (2010). Improved feature processing for iris biometric authentication system. *International Journal of Electrical, Computer and Systems Engineering, 4,* 127–134.

Deybach, G. (2007). Identity theft and employer liability. *Risk Management*, *54*(1), 14–17.

Douhou, S., & Magnus, J. R. (2009). The reliability of user authentication through keystroke dynamics. *Statistica Neerlandica, 63,* 432–449. doi:10.1111/j.1467-9574.2009.00434.x

Goldwasser, J., & Anderson, T. M. (2007). Passwords + pictures = security? *Your Money Kiplinger's,* June, 79–80.

Gorodnichy, D. O. (2009). Evolution and evaluation of biometric systems. *Proceedings of the IEEE Symposium on Computation Intelligence for Security and Defense Applications.* Retrieved from http://videorecognition.com/doc/publications/09-cisda-evol-eval-P.pdf

Gregory, A. (2008). Conserving customer value: Improving data security measures in business. *Journal of Database Marketing and Customer Strategy Management, 15,* 233–238. doi:10.1057/dbm.2008.20

Holtfreter, R., & Holtfreter, K. (2006). Gauging the effectiveness of US identity theft legislation. Journal of Financial Crime, 13, 56–64.

Jain, A., & Pankanti, S. (2001). Biometrics systems: Anatomy of performance. *Journal of IEICE, E00-A,* 1–11.

Jarillo, G., Pedrycz, W., & Reformat, M. (2008). Aggregation of classifiers based on image transformations in biometric face recognition. *Machine Vision and Applications, 19,* 125–140. doi:10.1007/s00138-007-0088-9

Kieke, R. (2009). Although a relatively new risk area, medical identity theft should not be taken lightly. *Journal of Health Care Compliance*, *11*(1), 51–54,73–74.

Kriemer, S. (2010). Matching the right patient to the right record: Biometrics on the rise as medical record security gets more attention. *Hospitals & Health Networks, 84,* 12.

Lafferty, L. (2007). Medical identity theft: The future threat of health care fraud is now. *Journal of Health Care Compliance*, *9*(1), 11–20.

Leong, L., & Yerzak, E. J. (2004). Password pitfalls and dynamic biometrics: Toward a multiplayer user authentication approach for electronic business. *Academy of Information and Management Sciences Journal, 7,* 21–25.

Maltoni, D., Maio, D., Jain, A., & Prabahakar, S. (2003). *Handbook of fingerprint recognition*. New York, NY: Springer-Verlag.

Mark, B. S., Debjani, B., Vijay, K., & Ernst, B. (2008). A proposed study and analysis of user perceptions of biometric acceptance. In (p. 3965). Retrieved from http://www.decisionsciences.org/proceedings/DSI2008/docs/396-2784.pdf

Marshall, C., & Rossman, G. (1999) *Designing qualitative research* (3rd ed.). Thousand Oaks, CA: Sage.

Marshall, P. (2007). *Identity theft: Limiting your employees' risk—and your liability.* Retrieved from http://hr.blr.com/whitepapers/Benefits-Leave/Employee-Benefits/Identity-Theft-Limiting-Your-Employees-Risk-And-Y/

McCollum, T. (2005). Flaws found in identity protection. *Internal Auditor, August,* 20–21.

Mercer, J. (2009). Breeder documents: The keys to identity. *Keesing Journal of Documents & Identity, 29*, 14–17.

Mercuri, R. T. (2006). Scoping identity theft. *Commmunications of the ACM, 49,* 17–23.

Monrose, F., & Rubin, A. (1999). *Keystroke dynamics as a biometric for authentication*. Retrieved from http://avirubin.com/fgcs.pdf

Newman, G., & McNally, M. (2007). *Identity theft research—A research review* [Abstract]. Retrieved from http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=210459.

Opperman, M. (2009). Red flag rules: are you ready? *Veterinary Economics, July,* 26-27.

Palaniappan, R. (2008). Two-stage biometric authentication methods using thought activity brain waves. *International Journal of Neural Systems, 18,* 59-66.

Perl, M. (2003). It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft. *Journal of Criminal Law and Criminology, 94,* 169–208.

Personix. (2006). *Secure healthcare banking: The critical step of identity verification* [White paper]. Retrieved from http://www.outputsolutions.fiserv.com/pdf/ HC_ Authentication _WP_v4.pdf

Podio, F., & Dunn, J. (n.d.). *Biometric authentication technology: From the movies to your desktop*. Retrieved from http://www.itl.nist.gov/div893/biometrics /Biometricsfromthemovies.pdf

Saunders, K., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers, & Technology, 13,* 183–192.

Schreft, S. (2007). Risks of identity theft: Can the market protect the payment system? *Economic Review, 92*(4), 5–40. Retrieved from ABI/INFORM Global database. (Document ID: 1447833331).

Schneider, G. (1997). Sarbanes-Oxley compliance: New opportunities for information technology professionals. *Academy of Information and Management Sciences Journal*, *10*(2), 79–89.

Schuckers, M.E. (2003). Using the beta-binomial distribution to assess performance of a biometric identification device. *International Journal of Image and Graphics, 3,* 523-529.

Smith, A.D. & Lias, A.R. (2005). Identity theft and E-fraud as critical CRM concerns. *International Journal of Enterprise Information Systems, 1,* 17-36.

Sullivan, R.J. (2009). Can smart cards reduce payments fraud and identity theft? Federal Reserve Bank of Kansas City, www.KansasCityFed.org, 35-64.

Sulovska, K. & Adamek, M. (2010). Research on Biometrical systems: an overview. Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, 21, 1463-1464.

Swartz, N. (2009). Will red flags detour ID theft? *Information Management, February,* 38-41.

van Kaam, A. (1959). Phenomenal analysis: Exemplified by a study of the experience of "really feeling understood". *Journal of Individual Psychology, 15*(1), 66–72.

Volner, R. & Bores, P. (2009). Biometric techniques in identity management systems. *Electronics and Electrical Engineering, 7,* 55-59.

Warren, C., & Drennan, T. (2008). Identity theft coverage unlikely under standard general liability policies. *National Underwriter,, 112*(38), 21–24.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). *Biometric systems, technology, design and performance evaluation*. New York, NY: Springer.

Wechsler, H. (2010). Intelligent biometric information management. *Intelligent Information Management, 2,* 499-511.

Wilcox, N. A., Jr., & Regan, T. (2002). *Identity fraud: Providing a solution*. Retrieved from http://www.lexisnexis.com/risksolutions/IdentityFraudWhitePaper.pdf

Winterdyk, J. & Thompson, N. (2008). Student and non-student perceptions and awareness of identity theft. *Revue canadienne de criminology et de justice penale, April,* 153-186. CJCCJ, DOI:10.3138/cjccj.50.2.153

Zhao, J. (2007). Identity theft . In B. S. Kaliski (Ed.) *Encyclopedia of business and finance* (Vol. 1, pp. 373–374). Detroit, MI: Macmillan Reference.