IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 9, Issue 3, July 2021

The Value of Biometrics in Protecting Financial Transactions Made Online

Dr. M V Rathnamma[1], S Riyaz Banu[2], Z Shoba Rani[3], Dr. V. Lokeswara Reddy[4]

Abstract:

The evolution of IT in the concept of online banking has made it easier and faster for account holders to transact online. When it comes to safeguarding one's financial identity, the legislation governing both technology and the financial sector must be considered. As a result, most modern online banks provide some level of transaction security upon customer entry to the login page of websites, along with a warning about the possibility of fraud. However, there has been an increase in the frequency of reports of online banking fraud. The customer's account might be hacked and used for fraudulent purchases on the internet. One of the most rapidly expanding subsets of consumer fraud is identity theft. Protecting the identities of consumers during international internet transactions necessitates the widespread use of biometric technologies like fingerprint scanning. Biometric technology is an example of cutting-edge engineering since it offers the possibility of using digital evidence for legitimate law enforcement purposes. This article employs a qualitative empirical legal research using a multidisciplinary research strategy by examining the norms set out in the Indonesian Law on Information and Transaction Electronic. In this study, we look at how biometric technology may be used to help prevent fraud using stolen identities in online banking. This research found that implementing biometric measures into financial systems is crucial. Biometrics may be used for electronic verification as hard proof of an authorized user's identity. As a Measure taken to safeguard its customers, it would support banking security measures.

Introduction

In spite of all the efforts of legislators and banks to make financial service law for consumer protection, however the consumer still has a vital role in protecting his or her financial information. Carelessness or lack of attention on the part of the consumer such as neglecting to protect passwords, disposing of identity information in regular trash, failing to secure regular mail or access to personal laptops, or responding to “phishing” attacks, can undo all the preventative work of governments and businesses [1].Case in Malaysia for example, Cyber Security Malaysia (CSM) had identified at least 900 unique phishing sites targeting financial institutions in the country, adding that it was quite easy for crooks to obtain personal information, usernames, passwords or credit card information through the phishing websites [2]. In the fact, scams targeting electronic banking have increased dramatically in the country, with the number more than doubling over the past year. In 2010, a total of 1,426 reports were made to CSM [3] compared with 634 in 2009 [4]. Recently in 2017, Malaysia investigating reported leak of 46 million mobile users' data [5]. In fact, it will impact to consumer trust when doing online transaction through online banking. If the crime increases and difficult to be overcame, the public trust for online banking will decrease automatically. It is a dilemma for online banking activities where identity theft frequently occurred, and then the identity can be used for doing cybercrime activities. It is a disadvantage of using “electronic” as medium transaction will impact to privacy and security risks [6]. Nowadays, identity theft is increasing at an alarming rate and is affecting millions of people [7]. There is not enough stringent methods are being adopted to protect customer accounts holder.

[1] Associate Professor, Department of CSE, K.S.R.M College of Engineering(A), Kadapa
[2,3] Asst. Professor, Department of CSE, K.S.R.M College of Engineering(A), Kadapa
[4]Professor, Department of CSE, K.S.R.M College of Engineering(A), Kadapa

ISSN 2347–3657
Volume 9, Issue 3, July 2021

According to a recent report by the US Federal Trade Commission, there is a new victim of ID theft every three seconds [8]. The parties of Bank, IT expert and legislator should work together to provide secure electronic transaction. Emergence of biometric technology development is expected to provide protection to consumer identity safer where the technology as an automated method of recognizing individual based on measurable biological and behavioral characteristics to identify the authorized user. Applying biometric technology for verification the consumer identity during online transaction will assist in providing the highest degree of security. Nowadays, the biometric technology can be used as identity government which is able to apply not only for personal information and business transaction but also for National security and law enforcement.

Research Methods

This research is a type of normative legal research. Normative legal research focuses on positive legal norms such as legislation. In addition, the study also principally derives from secondary law materials in the form of publications on cyber crime related to electronic information and transactions, including textbooks, legal dictionaries, legal journals, guides, directive or comments on related issues. The specification of this research is analytical descriptive, that is to describe, find legal facts thoroughly, and systematically study the problems that become the object of research

Result and Discussion

Cyber Crime and Online Identity Theft

There are many ways to steal personal information. In the fact, identity theft can be done both online ways and offline ways. Online ways can be done through such as, hacking activity, phishing emails, while offline ways can be done through shoulder surfing, and dumpster dives. Generally, hackers prefer steal personnel information through online way. Identity theft happens when fraudsters access enough information about someone's identity to commit identity fraud [9] where fraudsters can use it detail to do crime activity, such as take over customer existing account to obtain goods or services by deception. Identity is as personal information which must get protection from bank for not to be published to the general public. Refer to standard definition of personal information in most states of USA. Personal information defined as an individual's first name or first initial and last name plus one or more of the following data elements: (I) Social Security Number (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that include personal information [11]. Therefore, personal information shall not include publicity available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media [12]. Theoretically, there are two kinds of the unlawful. "Security breach" is typically categorized the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information [13], such as Phasing, Password cracking and Denial of service [14]. The breach focus on the technological process used to execute the attack. While, "computer crime" is generally broken into categories that emphasize the specific criminal activity taking place. Those crimes are typically categorized such as [15] Identity theft, Cyber stalking/Harassment, unauthorized access to computer systems or data, and Non-access computer crime [16]. In online way, computer crime can be called with cyber crime. There are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet [17]. Additionally, cyber crime also includes traditional crimes conducted through the Internet, such as online identity theft.

The Council of Europe's Cybercrime Treaty uses the term 'cybercrime' to refer to offenses ranging from criminal activity against data to content and copyright infringement [18]. The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access [19] in its cybercrime definition. In this regards, Symantec draws from the many definitions of cybercrime and defines it concisely as "any crime that is committed using a computer or network, or hardware device" [20]. Thus, a hacker can do cybercrime to steal online customer identity theft by this way. Therefore, in legal perspective, it needs cybercrime law approach [21]. The Oxford English Dictionary defines "identity" as "the set of behavioral or personal characteristics by which an individual is recognized". Thus, the traditional use of the word "identity" spoke

ISSN 2347–3657
Volume 9, Issue 3, July 2021

to one's name, familial membership, and occupation (among other applications) [22]. However, emergence of IT development, the meaning of "identity" traditionally has developed that extends meanings to include such things as one's consumer and credit histories, financial accounts, and Social Security number. It is a contemporary usage of "Identity" that is at issue when it comes to conceptualizing identity theft and identity crime [23]. Thus, personal information is as an identity to consumer.

While, the term of "identity theft" is the process of obtaining personal information that possible the perpetrator can pretend to be someone else. This is often done in order to obtain credit in the victim's name, leaving the victim with debt [24]. The term of "identity theft," most commonly thought of as the theft of an individual's personal identifying information, has evolved to include a new twist: business identity theft [25]. Thus, identity theft is the unauthorized access to personal information or other identifying information to commit fraud or other serious crimes [26]; while identity fraud is a crime involving the use of false identity [27]. The stolen identities use to unauthorized access of data, it refers to a scenario in which a person accesses data that he or she has not been given permission to access [28]. Furthermore, the data can be used to many other crimes. In fact, it is also sometimes difficult to investigate and to differentiate between authorized accesses and unauthorized [29].

Identity Theft through Phishing email

Identity theft scams via email or usually called with "phishing scam" is one of the activities in cyber crimes. The email sent will be appears as if come from a legitimate source such as a trusted business or financial institution, such as online banking. Frequently, it includes an urgent request message for personal information usually invoking some critical need to update their account immediately. The modus operandi is use technique through sending out millions of e-mails to users, often including advertisements for services and/or products with malicious viruses. In this case, consumer who unsuspectingly will automatically "clicked on" the link provided to fake banking website. In this situation, victims are hard to distinguish the fake website and original website. Then, perpetrator will persuade users to access the Web address that has been provided in order to read the message inside. By the online scams, perpetrator will steal consumer identity. In USA, approximately 40 percent of the frauds reported to the United States Federal Trade Commission (2007) over the last few years have involved some type of identity theft [30]. E-mail provider organizations report that as many as 85–90 percent of all e-mails are spam [31]. This fact makes the consumers should extra careful to avoid consumers are being victimized by cybercrime activity.

Identity Theft through Computer Hacking Activities

Computer hacking activities is a serious threat to consumer identity security. It is one of the ways that identity theft that can be done. A hacker can monitor all of consumer activities in online transaction through software assistance. A hacker can hack consumer personal computer and plant a spyware inside. A spyware is software that aids hacker in gathering information about consumer and that may send such information to hacker without the consumer's knowledge [32]. A hackers is not hard to bypass any run of the mill defense system, even at the consumer computer has installed antivirus, firewall or a combination of both [33]. Spyware could contain viruses which can be spread to user's computer while accessing an Internet site which contains the infected code or downloading something containing the infection. This virus allows hackers to gain control of your computer and steal any personal information.

Biometric Technology for Protecting Consumer Identity Theft

To protect "personal information" use traditional approach is very vulnerable. The consumer can be a victim in cyberspace. Authentication system which uses card, token or password systems is prone to be stolen or counterfeited. Thus, to provide consumer identity protection with high degree of security, bank must apply the internal policy. Nowadays, using biometric technology expected as effective way to protect financial transactions and against identity theft. As a special identity, individuals can be accurately identified by biometric technology [34] so that it will provide consumer identity theft protection. In digital edge, biometric technology can assist in authenticates an individual's identity automatically, and has several useful applications within Justice and Law Enforcement [35] including financial services law**.** In this regards, biometric technology has the ability to recognize fingerprint, iris, voice, facial recognition, hand, palm or skin. For example the use of fingerprint can assist to recognize authorize account holder of online banking. It can use in an effort to provide double security when doing online transaction. The system is also use to eliminate telecommunication crime.

In Pakistan, for example, SIM card vendors have been given three months to install biometric technology to confirm the identity of customers [36]. By using biometric technology will produce digital prints which it streamlines procedure to check and

ISSN 2347–3657
Volume 9, Issue 3, July 2021

cross-reference with multiple databases. In March, 1998, Malaysia has issued biometric passports. Furthermore, biometric data, such as thumbprint data was added to the biometric data on the passport chip in December 2002, it is similar technology that is used in the Malaysian identity card [37]. In 2011, Indonesia has a new policy related to the launch of e-ID. E-ID is equipped with microchip as data storage. This e-ID has an accurate identification method, so it applies internationally. The technology is also applicable in analyzing crime scenes, through fingerprint capture technology. This technology can capture, with a reasonable degree of accuracy prints and compare them against databases for identification. Thus, this technology provides transaction, data and web security when operating within databases as well as remote access to resources with mobile technology [38].

Biometric technology application is used for protecting consumer identity theft with high degree of security. Nowadays, the world of technology has advantages for securing consumer information and prevention of other potential threat on personal information. Online banking model has high security risk in providing consumer protection on online transaction. A bank must have internal regulation to lead their consumer to do transaction safely. It aims to avoid the use of customer identity for conducting illegal transactions by other parties. Therefore, data validation is very an important to ensure that a program operate on correct. It will be used to check for correctness, meaningfulness, and security of data that are input to the system [39]. In this regards, data validation will checks that data are valid, sensible, reasonable, and secure before they are further processed. In this regards, incorrect data validation can lead to data corruption so that the data may become inaccessible. Furthermore, the system or the related application will give an error. Thus, it leads to security vulnerable which allows an attacker to hack the system. The use of biometric technology application will help validate data more accurate because it use individual base which is embedded in human being. Application biometric technology provides double security while doing online transaction. Today, biometric validation can be implemented by bank for any transaction. Theoretically, definition biometric validation is "Services to support capturing extracting, comparing and matching a measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an entity. Biometric modalities include face, fingerprint, and iris recognition and can be matched on card, on reader or on server [40]. This paper identified two main benefits to apply biometric technology for consumer protection, as follows: **first,** Accuracy Data Validation. Bank security regulation is needed to lead consumer to access the system safely. Therefore, bank can regulate online transaction system through biometric data for validation. By using biometric data, it can be created a unique "key" which provides an added layer of security and control for authentication. It can be generated from hand, finger, retina and face. The use of fingerprint key for example, it can be used to unlock software capabilities, access to computers system and so on. To access the bank's system for an example, it will identify the customer through a high-resolution fingerprint recognition system that fits into a regular-size mouse. It will insure only the right fingerprint can access. In this situation, the bank will offer the mouse to its banking customers so that they can securely bank over the Internet. Special software will pass client authentication requests made using the mouse via a secure Internet link to the bank's Web server, where a centralized fingerprint template database will be housed [41]. By using biometric data validation, it will protect consumer identity theft with accuracy is around 99.9% [42]. Thus, data validation without biometric data is difficult to detect unauthorized user. The use of advanced technology to identify individual base will prevent consumer identity theft for account takeovers. In practice, the biometric technology can be installed in Smartphone, so biometric data such as finger, face and voice recognition will facilitate the implementation of the online transaction safely. It will replace traditional authentication method, such as "passwords" and "usernames". Biometric data will support law enforcement through real evidence.

Second, Data Manipulation Protection. A large number of identity theft cases occurred through computer hacking activities. Hackers steal personnel information through online ways. Generally, hacker will attack computer that don't have firewalls and anti-virus software installed [43]. Therefore, bank must have policy to regulate up-date the bank security system. In online banking, firewall is an essential part for using as a filter. It is either a software program or hardware device used in computer systems to prohibit forbidden information for passing though, while allowing approved information. The communication which the firewall prevents from passing though could be hackers trying to gain access to your personal information stored on your computer [44]. The data base in bank's computer system without firewall is high risk for identity theft. However, a hacker can still easily circumvent firewall blocking techniques. File transfer Protocol (FTP) servers can use a different port, and website can act as gateways to blocked sites without

detecting by firewall [45]. In fact, stealing a consumer's password is one of the biggest fraud scams plaguing banks. Thus, by implementing biometric technology, it would be difficult for hacker or fraudsters to steal and to manipulate an account holder identity. In this regards, biometric would prevent many instances because it is as an automated method of recognizing individual based on measurable biological and behavioral characteristics to identify the authorized user. Consumer protection will more effective by using own human characteristics. While, use of traditional authentication is high risk for data modification, so that the perpetrator can change password and PIN easily to do transaction as if the user is authorize person. Thus, biometric technology will help to minimize an effort of data manipulation. Increasing of mobile payments for goods and services through online transaction, it makes verifying process for consumer identity could be more important to minimize frauds. Biometric technology could play a key part in the authentication process before the transaction took place. In this regards, bank has play role in an effort to protect consumer identity theft through making internal regulation on training and education for consumer while doing online transaction in order to avoid cyber crime. Bank must update regularly the security system and e-verification tools for supporting online and mobile banking activities safely.

Conclusions

This article identified biometrics technology as a potential safeguard against common forms of online identity theft including phishing and hacking. When applied to the realm of consumer identity protection, biometric technologies promise an unprecedented level of safety. This research found that implementing biometric measures into financial systems is crucial. In this context, biometrics technology will validate data with high precision, helping to identify illegal users with hard proof. The system will recognize a person based on observable biological and behavioral traits to identify the authorized user, which will prevent the identity of the consumer being stolen and manipulated by a hacker.

References

[1] Norm Archer, (2011), "Consumer identity theft prevention and identity fraud detection behaviors", Journal of Financial Crime, Vol. 19 is: pp. 20 – 36, http://dx.doi.org/10.1108/13590791211190704, [accessed 05.04.2019].

[2] The Star newspaper (2011), E-banking scams on the rise, Wednesday February 16, 2011. http://www.thestar.com.my/news/story.asp?sec=nation&file=/2011/2/16/nation/8071653, [accessed 08.06.2018].

[3] Cyber Security Malaysia is positioned as the national cyber security specialist under the Science, Technology and Innovation Ministry, and operates the Cyber999TM Help Centre for local Internet users. See on www.cybersecurity.my, [accessed 08.06.2018].

[4] He Star newspaper, E-banking scams on the rise, loc.cit.

[5] Reuter, Malaysia investigating reported leak of 46 million mobile users' data, https://www.reuters.com, [accessed 27.08.2019]

[6] See also Alan Davidson (2009), The Law of Electronic Commerce, Cambridge University Press, Sydney, p.1

[7] Biometric are key for secure banking (2013), http://www.biometricupdate.com. [Accessed 02.10.2018].

[8] David I. Bainbridge (2008), Introduction to Information Technology Law, Pearson Longman, six editions, England, p. 504

[9] Identity fraud and identity theft (2013), http://www.actionfraud.police.uk/, [accessed 02.10.2018]