CONSUMER IDENTITY THEFT PROTECTION IN ONLINE BANKING TRANSACTION THROUGH BIOMETRIC TECHNOLOGY APPLICATION

By Edy Santoso

Nusantara Islamic University

ABSTRACT

The development of information technology in online banking model provides efficiency and effectively for account holder to do online transaction. In this situation, technology and financial services law plays important role in providing consumer identity protection. Nowadays, the most of online banks offer transaction safety when consumer access to login page of websites to warn users about the existence of such scams. However, the cases of online banking scams have been increasing from time to time. Perpetrator can access to the consumer's account and do online transaction illegally. Identity theft is one of the fastest growing types of consumer fraud. In this regards, using biometric, such as fingerprint technology is very important to protect the consumer identity during online transaction in over the world. Thus, biometric technology can be used for real evidence in law enforcement at cyberspace. By multidisciplinary approach, this paper examined consumer identity theft protection in online banking transaction through biometric technology application. The result show that the biometrics technology can be applied for e-verification as real evidence in detecting authorized user. In legal aspect, there are three approaches for protecting consumer identity through approaching to banking security regulation on biometric validation, approach to government regulation on consumer identity protection and approach to consumer behavior on keeping identity.

Keyword: Consumer Identity Protection, Biometric Technology, online banking, online scams, identity government.

1. 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 personal 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].

The fact 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 [5].

Nowadays, identity theft is increasing at an alarming rate and is affecting millions of people [6]. There is not enough stringent methods are being adopted to protect customer accounts holder. According to a recent report by the US Federal Trade Commission, there is a new victim of ID theft every three seconds [7].

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.

At this time, fingerprints and samples had been lawfully as evidence. In UK it regulated under section 64 (1A) of the Police and Criminal Evidence Act 1984. The aim of the underlying policy was the prevention and detection of crime, the investigation of offences, facilitating prosecutions and exculpating the innocent and dealing with miscarriages of justice [8].

Applying biometrics technology in online banking activities, it could be to become a “double security” when use electronic transaction where there is not only input “password” and “PIN” but also input ”biometric” identity. Therefore, it is very important to examine personal identity protection in online banking transaction through application biometric technology from legal perfective.

2. 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 [10].

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 [11].

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 [12], such as Phising, Password cracking and Denial of service [13]. 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 [14] Identity theft, Cyber stalking/Harassment, unauthorized access to computer systems or data, and Non-access computer crime [15].

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 [16]. 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 [17]. The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access [18] 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” [19].

Thus, a hacker can do cybercrime to steal online customer identity theft by this way. Therefore, in legal perspective, it needs cybercrime law approach [20]. 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 to one’s name, familial membership, and occupation (among other applications) [21]. 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 this contemporary usage of “identity” that is at issue when it comes to conceptualizing identity theft and identity crime [22]. 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 [23]. 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 [24]. Thus, identity theft is the unauthorized access to personal information or other identifying information to commit fraud or other serious crimes [25]; while identity fraud is a crime involving the use of false identity [26].

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 [27]. 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 [28].

2.1. 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 [29]. E-mail provider organizations report that as many as 85–90 percent of all e-mails are spam [30]. This fact makes the consumers should extra careful to avoid consumers are being victimized by cybercrime activity.

2.2. 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 [31]. 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 [32].

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.

3. 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 [33] 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 [34] 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 [35]. By using biometric technology will produce digital prints which it streamlines procedure to check and 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 [36].

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 [37].

Biometric technology application is used for protecting consumer identity theft with high degree of security. In legal aspect, this paper examined three approaches for consumer protection, as follows:

3.1. Approach to Banking Security Regulation On Biometric Validation

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 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 [38]. 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 [39].

3.1.1. 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 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 [40].

By using biometric data validation, it will protect consumer identity theft with accuracy is around 99.9% [41]. 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.

3.1.2. 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 [42]. Therefore, bank must have policy to regulate up-date the bank security system.

In online banking, firewall is 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 [43].

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 [44].

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.

3.2. Approach to Government Regulation on Consumer Identity Protection

This paper will examine Malaysia regulation in providing consumer identity theft in online banking. Nowadays, Malaysia’s Personal Data Protection Act 2010 (PDPA) has regulated the processing of personal data in the context of commercial transactions by data users, and providing a safeguard for the interests of data subjects.

However, this Act has not been regulated personal data for email scams which is frequently for identity theft activities occurred. Thus, this Act has not been protected consumer of financial data for identity theft through email scam specifically.

In this regards, perpetrator of email scam usually posing as a financial institution sends spoof e-mails to a number of possible victims requesting verification or an update of their account details. The link incorporated in the e-mail redirects the recipient to a counterfeit webpage designed by the cyber criminal, which closely replicates that of a legitimate financial institution [45]. “Phishing”, which it is a short form of ‘password harvesting fishing’ and refers to a particular method of online identity theft.

This Act has some principles which are able to protect consumer’s personnel data in cyber space. There is disclosure principle that said “No personal data shall be disclosed without the consent of the data subject, be disclosed the purpose for which the personal data was to be disclosed at the time of collection of the personal data [46]. Thus, disclose the personnel data without permission is violation.

Furthermore, the Act has applied security principle that said “A data user shall take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction [47]”. In the regards, unauthorised access is very important issue in e-mail scam. Consumer should protect themselves. Because, if consumer to disclose security information, perpetrator will copy all of victim’s personal financial data and do identity fraud.

Generally, victim never rechecks whether the e-mail is spam or not. In the context of online banking activities, this Act provides personal data protection for unauthorised access and misuse into customer's bank account. This section is very important to protect personnel financial information because unauthorised access to the customer's banking system allows a perpetrator to do identity theft activity.

In this situation, the bank security system has play important role to protect the crime. Validation data for authorize user very important to avoid hacking activities which will steal the consumer identity. Therefore, this Act must adopt and regulate the biometric technology to assist e-verification properly in online banking activities.

To anticipate cybercrime activities which are done by hacker, Malaysia's Computer Crimes Act 1997 has regulated about secure access to any program or data held in a computer. Section 5.(1) said that "A person shall be guilty of an offence if he modification of the contents does any act which he knows will cause unauthorised of any computer. Thus, this section is aim to provide protection of consumer financial information which is caused of modification of the contents of any computer" which is usually done by a hacker to copy and modify the data.

This Act is very important to protect consumer financial information for criminal activity which is done by black hat hacker (cracker). A cracker would be very dangerous because they can penetrate the computer systems of banks and then hacker is not only able to steal consumer identity but also is able to modify consumer data. Thus, this Act can be applied to combat computer crime on hacking activities.

However, these Act should harmonized with Malaysia's Consumer Protection Act 1999 because it has not been set up specifically on email scam. This Act more focused on consumer protection in traditional transaction. It just regulates the safety standard in relation to goods may relate to the performance, composition, contents, manufacture, processing, design, construction, finish or packaging of the goods [48].

This legislation is only to provide basic protection for consumer. Section 2.(2).(g), said " This Act shall not apply to any trade transactions effected by electronic means unless otherwise prescribed by the Minister [49]". However, in electronic transaction, Malaysia's Digital Signature Act 1997 is very important to protect illegal transaction which is conducted by perpetrator.

By using an asymmetric cryptosystem such that only a person having the initial message and the signer's public key from bank who can doing transaction. It means, if the identity theft happened, a perpetrator cannot do electronic transaction only by using "user name" and "password". Consumer will get confirmation is any electronic transaction first before is executed. However, it need time to get confirmation that usually sends to mobile phone.

Therefore, this Act should consider biometric technology to ensure that the user is an authorized person when doing transaction. It is not only use digital technology for verification but also use biometric data will assist the bank recognizes the authorize user properly.

3.3. Approach to Consumer Behavior on Keeping Identity

The banking sector environment is especially vulnerable to a wide range of cyber threats. Those in charge of information security have been investing significant resources into the implementation of diverse technologies designed to protect both data and information technology (IT) infrastructure from those threats.

However, today's highly IT-dependent financial institutions are till insufficient for providing safeguard for online transaction. Overreliance on security technology can put a financial institution at risk because a large percentage of information security breaches are in reality the outcome of flawed human behaviors, rather than hardware or software weaknesses [50].

Therefore, it is not only bank and government that has plays important role in protecting consumer but also consumer behavior themselves has the same role. Online banks should has internal regulatory and security system to guide the consumer so that they can verify and do transaction securely.

In cybercrime, by using phishing site with similar domain name, it is easy for perpetrator to do identity theft. It was professionally designed and difficult to identify, especially for beginner in online banking transaction. When someone clicks the link, user will visit the fake Web site. When the victim enters his or her login information to "verify" the account, that person provides the perpetrator with his or her username and password. The perpetrator can then log on to the victim's real account and steal funds [51].

In this situation, it is very important for consumer behavior, and controls their emotion when getting "surprising email" in order to avoid e-mail scam. Thus, consumer is not to follow links that have been e-mailed. It is important for consumer to recheck. Consumer should contact the bank to verify if the e-mail is genuine. It is understand that no anti-virus can give us one hundred percent protection for email scams.

Therefore, the most effective protection for consumer identity theft is to develop the consumer's right habit. Costumer need to learn and practice these safe surfing habits. Furthermore, it is very important for consumer to follow what bank has provided equipping and training. Bank need provide educating customers on their role in maintaining security of banking information and remind consumer for risks involved in using online banking. Thus, consumer has a vital role in protecting his or her personal information.

4. CONCLUSION

In general, this paper indentified that biometrics technology expected to protect consumer identity theft from cyber crime actives that is committed using a computer or network, or hardware device to do online illegal activities, such as phishing email and hacking activity as usual practice. Biometric technology application will provide high degree of security for consumer identity protection.

This paper examines three approaches for providing protection consumer identity theft from legal aspect. **Firstly**, approach to banking security regulation on biometric validation. In this regards, biometrics technology will provide accuracy data validation, where it will assist to detect unauthorized user through real evidence. Then, it also will provide protection from data manipulation, where it will prevent consumer identity for an effort of hacker to steal and manipulate it because the system will recognize individual based on measurable biological and behavioral characteristics to identify the authorized user. **Secondly**, approach to government regulation on consumer identity protection. Although, the Malaysian government regulation has regulated data protection, but some Act which relate to online transaction and computer crime must harmonized each other and considering adopting biometrics technology application, particularly e-verification in online transaction. **Thirdly**, approach to consumer behavior on keeping identity. Customer behavior is play important role in prevent their identity. There is no one hundred percent guaranty of using hardware and software can protect consumer identity from cyber crime. Bank must have internal regulation which can lead consumer to involve in maintaining security of banking information through providing equipment and training regularly.

REFERENCES

[1] Norm Archer (2011(, "Consumer identity theft prevention and identity fraud detection behaviors", Journal of Financial Crime, Vol. 19 Iss: , pp. 20 – 36, http://dx.doi.org/10.1108/13590791211190704, [accessed 05.09.2012].

[2] See 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 08.06.2011].

[3] See 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 08.06.2011].

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

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

[6] Biometric are key for secure banking (2013), http://www.biometricupdate.com/201308/biometric-are-key-for-secure-banking. [accessed 02.10.2013].

[7] *Ibid*

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

[9] *See* also Identity fraud and identity theft (2013), http://www.actionfraud.police.uk/fraud_protection/identity_fraud, [accessed 02.10.2013].

[10] See Data Breach Charts (2013) , Bakerhostetler, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf, [accessed 02.10.2013].

[11] *Ibid*

[12] *Ibid*

[13] Chuck Easttom and Det.Jeff Taylor (2011), *Computer Crime, Investigation, and the Law* , Course Technology, Boston, p.3.

[14] Chuck Easttom and Det.Jeff Taylor, *Ibid*, 4

[15] Chuck Easttom and Det.Jeff Taylor, *Ibid*, 4

[16] See Cyber crime (2013), accessed October 16, 2013, http://www.webopedia.com/TERM/C/cyber_crime.html. [accessed 16.10.2013].

[17] Krone, T., 2005. *High Tech Crime Brief.* Australian Institute of Criminology (Canberra, Australia, 2005). ISSN 1832-3413.

[18] United Nations, 1995

[19] What is Cybercrime? (2013), http://us.norton.com/cybercrime-definition, [accessed 16.10.2013].

[20]Substantive cybercrime laws is including, laws prohibiting online identity theft, hacking, intrusion into computer systems, child pornography, intellectual property, online gambling.

[21]Judith M. Collins (2005), *Preventing Identity Theft in Your Business How to Protect Your Business, Customers, and Employees,* John Wiley & Sons, Inc., New Jersey. p.7.

[22] Judith M. Collins, *Ibid*

[23] Judith M. Collins, *Ibid*, 5

[24] Judith M. Collins, *Ibid*, 8

[25] See Albrecht, W.S., Albrecht, C.C., Albrecht, C. and Zimbelman, M. (2011), Fraud Examination, South-Western Cengage Learning, Mason, OH. See also Norm Archer, ,"Consumer identity theft prevention and identity fraud detection behaviours", Journal of Financial Crime, Vol. 19 (2011) Iss: 1 pp. 20 – 36, http://dx.doi.org/10.1108/13590791211190704, [accessed 05.09.2012].

[26] See Sproule, S. and Archer, N. (2007), “Defining identity theft”, 2007 World Congress of the Management of e-Business, IEEE Computer Society, Los Alamitos, CA, pp. 163-73. See also Norm Archer, "Consumer identity theft prevention and identity fraud detection behaviours", 21.

[27] Chuck Easttom and Det.Jeff Taylor, *Op.Cit*, p. 12.

[28] See *Ibid*, p. 19.

[29] Norm Archer,"Consumer identity theft prevention and identity fraud detection behaviours", *Op.cit*.

[30] Zaenab Karake Shalhoub and Sheikha Lubna Al Qasimi (2010), *Cyber Law and Cyber Security in Developing and Emerging Economies.* Edwar Elgar, USA, p. 37.

[31] *See also* Spyware Workshop, Monitoring Software on your PC, Spyware, Adware, and Other Software, Staff Report, Federal Trade Commission, 2005.

[32] See also Elinor Cohen, The ways perpetrators steal identities – Part II in the Identity Theft series, posted on 2 May 2013, http://www.cyber-dome.com/the-ways-perpetrators-steal-identities-part-ii-in-the-identity-theft-series/, , [accessed 15.10.2013].

[33] See What are the benefits of biometric technology?, http://www.ibia.org/biometric/faq/, [accessed 02.10.2013].

[34] *Justice and Law Enforcement Biometric* (2013), http://findbiometric.com/applications/justicelaw-enforcement/, [accessed 12.02.2013].

[35] *Pakistan to introduce biometric controls for SIM card sales*, http://www.planetbiometric.com/article-details/i/1372/. [accessed 12.02.2013].

[36] http://en.wikipedia.org/wiki/Malaysian_passport, [accessed 12.02.2013].

[37] *Justice and Law Enforcement Biometric, Op.cit*

[38] *See* Data validation, http://en.wikipedia.org/wiki/Data_validation, [accessed 12.10.2013].

[39] Executive Office of the President, Federal Identity, Credential, and Access Management (FICAM) Roadmap and implementation Guidance, at 35 (Ver.1.0) (Nov.10. 2009), Powered by the Federal Chief Information Officers Council and the Federal Enterprise Architecture.

[40] Biometric in Banking, Fingerprinting Through the Mouse, http://www.bankersonline.com/articles/bhv09n12/bhv09n12a2.html, [accessed 12.02.2013].

[41] *See* Biometric are key for secure banking, http://www.biometricupdate.com/201308/biometric-are-key-for-secure-banking . [accessed 02.10.2013].

[42] *See also* Computer Hacking and Identity Theft, http://www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx, [accessed 02.10.2013].

[43] What is a firewall? , http://www.checkpoint.com/resources/firewall/. [accessed 13.10.2013].

[44] *See also* Kevin Hamel, Three Pillars of Bank Network Security, accessed October, 13, 2013, http://www.cocc.com/bank-network-security.html, [accessed 13.10.2013].

[45] See also Zaenab Karake Shalhoub and Sheikha Lubna Al Qasimi, *Op.cit*, 41.

[46] S.8 (1) Personal Data Protection Act 2010

[47] S.9 (1) Personal Data Protection Act 2010

[48] S.19 Consumer Protection Act 1999

[49] S.2.(2).(g) Consumer Protection Act 1999

[50] See Zaenab Karake Shalhoub and Sheikha Lubna Al Qasimi, *Op,cit*, 35.

[51] Chuck Easttom and Det.Jeff Taylor, *Computer Crime, Investigation, and the Law*, *Op.cit*, p. 7.