CONSUMER PROTECTION FOR ONLINE BANKING SCAMS VIA E-MAIL IN MALAYSIA

Edy Santoso[1]
Universiti Utara Malaysia
Universitas Islam Nusantara

Abstract

The new advancement in technology both hard and soft is creating new opportunities for cyber criminals. It is an effective tool for going against the law. In the economic sector, the number of Malaysians opting for online banking to do transaction is increasing. There are 9.8 million online banking account holders in Malaysia. However, cases of online banking scams in Malaysia have been increasing since such first case was registered in 2005. Statistics from Financial Mediation Bureau showed that the number of cases had increased. Therefore, the objectives of this paper are to identify cyber scams via email in online banking business model and to examine consumer protection of online banking scams in Malaysia.

Keywords: Online banking scam, email scam, phishing website

Introduction

In line with the increasing use of the Internet as a business tool, the case of cyber crime from time to time shows an increase. Financial and cyber crimes are the most common crimes committed in Malaysia.[2] Statistics from Financial Mediation Bureau (FMB) showed that the number of cases had increased from only 46 in 2008 to 163 in 2010.[3] It means the crime have jumped nearly four times for only 2 (two) years period.

1 Visiting Senior Lecturer at Universiti Utara Malaysia from 2010-2012 and senior lecturer at Universitas Islam Nusantara, Bandung, Indonesia.

2 Tommy Seah, "Cyber Crime Tops List of Most Common Crimes in Malaysia, Cyber Crime Cyber Security Malaysia," http://www.thenewnewinternet.com/2010/04/15/cyber-crime-tops-list-of-most-common-crimes-in-malaysia/ (accessed June 11, 2011)

3 P. Aruna, "Don't fall prey to online banking scams," *The Star Newspaper*, Saturday February 19, 2011, http://thestar.com.my/news/story.asp?file=/2011/2/19/nation/8039959&sec=nation (accessed June 5, 2011).

Modus operandi of the scams begins with the way to send email spam to consumers. The e-mail will state that receivers need to log in immediately and to update their contact information for security purposes. Those who fall prey for these scams are usually new Internet banking account holders and those who lacked a general understanding of Internet security and they are not aware that such scams exist.

The trap was to trick Internet banking account holders into revealing their online banking username and password. They use fake banking websites, known as "phishing" sites to try and trap the account holders. This fake websites are used to mislead users into logging in by entering their usernames and passwords, which are immediately copied by the creator of the site. The cyber criminal then can log in and withdraw the users' entire account.

The highlight issue in this situation is that the victim of online banking scam could not compensate for their losses. Thus, customer protection on online banking in Malaysia is still vulnerable. In this situation, the local bank will refuse to offer a refund.[4] This case will be associated with how the protection of consumers that can be anticipated by the bank, so that the consumers are not harmed by the crime.

In this regards, there are very complicated legal cases in the use of the Internet as a business tool today. Legal efforts should be made to get customer money back which is caused by the weakness of the electronic transaction system in online banking. There were 163 cases last year, but only 51 victims managed to get part or all of their money back.[5]

Methods/Approach

This paper uses legal research with multidisciplinary research approach through the analysis of legal rules under Malaysian Law.

4 Aruna, "Don't fall prey to online banking scams," n. 3.
5 Aruna, "Don't fall prey to online banking scams," n. 3.

A. Cyber scams via email in online banking business model

In line with the growth of Internet usage, Internet crime is also growing rapidly. Internet usage has created a lot of problems such as people are tricked into providing personal information such as credit card numbers, passwords, Mother's maiden name, bank account numbers, ATM pass codes and social security numbers. In this situation, virus protectors and firewalls do not catch most phishing scams because they do not contain suspect code, while spam filters let them pass because they appears to come from legitimate sources.[6]

In this situation, cyberspace allows facilitating stolen identities activities. The stolen identities can be used to unauthorized access; it refers to a scenario in which a person accesses data that he or she has not been given permission to access.[7] Furthermore, the data can be used in many other crimes. In the fact, it is also sometimes difficult to investigate and to differentiate between authorized accesses and unauthorized.[8]

Theoretically, computer crimes will always involve some type of "computer-security breach". It is not synonymous with "computer crime". Those breaches are typically categorized as follows (or something very similar):[9] Privilege escalation, Malware (Trojan horse, virus, worm, logic bomb, root kit, etc), Phising, Social engineering, Session hijacking, Password cracking and Denial of service. While, computer crime is generally broken into categories that emphasize the specific criminal activity taking place rather than the technological process used to execute the attack. Such list would be similar to the following:[10] identity theft, cyber stalking/ Harassment, unauthorized access to computer systems or data, and non-access computer crime.

---

6 What Is a Phishing Scam? http://www.wisegeek.com/what-is-a-phishing-scam.htm (accessed February 22, 2011).

7 Chuck Easttom and Jeff Taylor, *Computer Crime, Investigation, and the Law* (USA: Course Technology Cengage Learning PTR, 2011), 12.

8 Easttom and Taylor, *Computer Crime, Investigation, and the Law*, 19.

9 Easttom and Taylor, *Computer Crime, Investigation, and the Law*, 3.

10 Easttom and Taylor, *Computer Crime, Investigation, and the Law*, 4.

Identity theft is the process of obtaining personal information so that 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.[11] The U.S. department of Justice defines identity in this manner:

> "*Identity theft and identity fraud" are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain*".[12]

While, the Oxford English Dictionary defines "identity" as "the set of behavioral or personal characteristics by which an individual is recognized. In this regards, the meaning of identity theft is to be distinguished from identity crimes those offenses committed using the stolen personal or business identifying information or "identities." Thus, the conceptual relationship between identity theft and identity crime is that the former facilitates the latter.

There are some legal problems which are identified as cyber scams activities via email in online banking business model, as follows:

1. Email Scam

Nowadays, cyber criminals via email scams is a kind of *modus operandi* by sending out millions of e-mails to users, often including advertisements for services and/or products with malicious viruses. The first spam e-mail appeared in 1978, but the frequency and maliciousness of spam have increased dramatically. Today, e-mail provider organizations report that as many as 85–90 percent of all e-mails are spam.[13]

---

11 Easttom and Taylor, *Computer Crime, Investigation, and the Law*, 5.

12 What Are Identity Theft and Identity Fraud? http://www.justice.gov/criminal/fraud/websites/idtheft.html (accessed May 10, 2013).

13 Zeinab Karake Shalhoub and Sheikha Lubna Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies* (USA: Edward Elgar Publishing, 2010), 37.

Surprisingly, it has been estimated that the response rates to this kind of spam e-mail range from 0.5 percent to 4 percent.[14] This fact is disturbing, given the frequency with which the phishing attacks are unleashed. Furthermore, Symantec (2007) reports that in the first half of 2007, its software blocked over 2.3 billion phishing messages.[15]

In 2008, it was full of stories of cyber criminal activities all around the world, with hackers, spammers, and phishers causing chaos, and, in some cases, confusion on computer systems and consumers, causing credit and debit fraud numbers to soar. Experts and law enforcement officials worldwide who hunt down cyber crimes state that scams increased in the last half of 2008, as criminals took advantage of economic uncertainty and unease to attack both consumers and businesses.[16]

In this situation, fraud is becoming part of cyber activities. No wonder what are logic rules behind every crime pattern but the end result is fixed which means their only financial gains.[17] Thus, fraud is able to be part of computer crime which is very easy to do in cyberspace. It is very difficult to control this crime because it is conducted easily anywhere and anytime. Thus, it can also capture victims worldwide.

Once the account details are disclosed, the cyber criminal will use them fraudulently to enrich himself/herself.[18] This crime model called "phishing", which it is a short form of 'password harvesting fishing' and refers to a particular method of online identity theft.

As the Internet usage in the country grows, the total number of online transactions along with other activities is likely to increase. It is in line with the increasing number of online crime incidences. Growth in broadband and wireless capacity makes the Internet more

14 Bielski, L. "Phishing phace- off: Online fraudsters and vendors do battle to gain control of electronic information," *ABA Banking Journal* 96, no.9 (2004): 46.

15 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 41.

16 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 37-38.

17 How to Report Fraud and Scams, http://www.419legal.org/blog/2010/04/12/how-to-report-fraud-and-scams/ (accessed February 22, 2011).

18 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 41.

convenient and quicker to use. Unfortunately, these utilities could be used as means for increasing cyber crimes.

It is worrying, according to International Data Corporation (IDC) survey in Malaysia, the number of Internet users will increase to 18.5 Million and number of online spending will increase to 10.5 Million by 2012. As per survey of International Data Corporation (IDC) in 2007, the overall e-commerce spending in Malaysia was US$22.3 billion which is expected to get doubled by 2012.[19]

The problem of insufficient awareness about cyber security among Malaysians surfing on the Web continues to pose a big challenge. For example, some users do not own a distinct password while many are not updating their security software.[20] Therefore, it is hardly surprising that online crimes involving banking fraud and phishing rose 619% in 2008 over 2007.[21]

2. Typo squatting

This crime is using strategy of likelihood of confusion of a similar domain name. Generally, this *modus operandi* will use the link to email spam which has been sent to the victim. Consumer will "click" automatically the domain name address which appears at email spam. It is very difficult for the victim to dedicate this because it has a design similar to a legitimate online financial institution.Thus, frequently Internet banking becomes the easy target of cyber crime.

Besides, the crime *modus* is quite unique and victims are often not aware of it. Crime perpetrators create a nearly identical site to the site of potential victims. For example, a website address http://www.balicash.com may be faked with an address http://www.balikas.com or even http://www.balicash.net or similar name. It is almost hard to see the difference. In this situation, the typosquatter will register a fake domain name which is designed to make typographical errors when accessed by consumer.

19 E-commerce in Malaysia, http://www.getranked.com.my/e-commerce/e-commerce-in-malaysia.html (accessed October 20, 2012).

20 Malaysia Experiencing Rise in Cyber Crimes, http://www.spamfighter.com/News-11776-Malaysia-Experiencing-Rise-in-Cyber-Crimes.htm (accessed June 11, 2011).

21 Malaysia Experience Rise in Cyber Crimes, n. 20.

When registered, the automated system does not review for similarities in domain names. Consequently, the system computers would automatically register both "businessclient.com" and "business-client.com" as two completely different domain names.[22] Therefore, it is very important for the trademark owner to register their trademarks as domain name.

In searching of website address through "search engine", this crime will involve the scenario through 'mouse trapping', where expects Internet users will make mistakes misspelling when typing website. In this regards, domain name infringement by cybersquatters weakens the fundamental trademark principle of consumer protection by permitting ruthless competitors to benefit from the mark holder's good will and reputation.[23]

In this situation, typosquatting can be easily created top-level domains such as **.**com, .net and .org domains. Everyone may name a site whatever they like as far as the domain is not yet owned by somebody else. It is more dangerous if this case is done in online banking activity. Typosquatter aims to get financial information, which will be used to perform illegal transactions. For example, in 2001 there was a case in Indonesia on Internet banking of the Bank Central Asia (BCA) site, *www.klikbca.com* being duplicated with 5 (five) similar domain names.

The illegal website appears on similar site with the original one. This caused the User PIN and Password number to be recorded at the site. Unfortunately, this case was settled via alternative dispute resolution due to the absence of a specific regulation in cyberspace at the time in Indonesia. Perhaps this scenario could be equated to the principle of legality which is a fundamental rule in criminal law that nothing is a crime unless it is clearly forbidden by law.[24]

---

22 Dara B. Gilwit, *The Latest Cybersquatting Trend: Typosquatters,Their Changing Tactics, and How To Prevent Public Deception and Trademark Infringement*, http://law.wustl.edu/Journal/11/p267Gilwitnotebookpages.pdf, p.6 (accessed July 12, 2011).

23 Gilwit, *The Latest Cybersquatting Trend*, 9.

24 Definition of the principle of legality see http://www.businessdictionary.com (accessed May 10, 2013).

3. Phishing Scams

Due to such similar domain names, perpetrators may create a website which is similar to the original website. Fake banking websites, known as "phishing" sites, to try and trap the account holders.[25] The websites are used to mislead users into logging in by entering their usernames and passwords, which are immediately copied by the creator of the site. The cyber criminal, then can log in and empty the users' entire account in minutes if the amount is within the limit allowed to be transferred in a day. Users do not know if the website that they have accessed is fake website with similar Domain name.

The email sent would appear as if it came from a legitimate source such as a trusted business or financial institution. It includes an urgent request for personal information usually invoking some critical need to update an account immediately. Consumer who unsuspectingly will automatically "clicked on" the link provided to fake banking website.

The links included in phishing scams take the unsuspecting person to a fraudulent website designed to mimic the real thing, often down to the smallest detail including copyright notices, submenu titles and so on. It's virtually impossible for most people to tell they are the target of a phisher by looking at the site alone.[26] In this regards, many Internet users especially beginners, tend to believe everything they read in his/her e-mails inbox and become easy prey to cyber criminals out to steal their personal and financial information.

Accordingly, foreign banks, especially those in Eastern Europe and Brazil, have applied more technologically based, radical measures to secure their online banking operations; it is indicated that, as a result, almost 100 percent of Brazilian Internet banking depends on secure website protocols and uses two personal identification log-in requirements.[27]

---

25 P. Aruna, "Rise in scams targeting e-banking accounts," *The Star Newspaper*, Wednesday February 16, 2011http://thestar.com.my/news/story.asp?file=/2011/2/16/nation/8073924&sec=nation (accessed June 5, 2011).

26 *What Is a Phishing Scam?*, http://www.wisegeek.com/what-is-a-phishing-scam.htm (accessed June 5, 2011).

27 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 36.

In September 2007, Deloitte surveyed 169 worldwide financial institutions on operational security and reported that standard, basic security measures such as encryption, access control, and network security are insufficient at protecting banking and financial institutions' online operations. The survey determined that 27 percent of respondents had become victims of security breaches in their international operations in 2007.[28]

Furthermore, according to Norton's report recently, "up to 83 percent of Internet users in Malaysia have fall victim to cybercrimes".[29] Phishing-related crimes can be particularly difficult to investigate for a number of reasons. First, victims are often unaware a crime has been committed until long after it has occurred. Second, skilled identity thieves know how to hide their tracks. Moreover, they will conduct the phishing operation only for a limited time and then shut it down.[30]

B. Consumer Protection of Online Banking Scams in Malaysia

Legislation, investigations, and the prevention of identity theft can take different approaches, depending on the type of the identity stolen. Thus, to mitigate and prevent identity thefts requires that each type of identity be clearly delineated: personal, business, and overarching.[31] In other words, personal identity theft is the unauthorized acquisition of another individual's personally sensitive identifying information.[32] Personal identity crime itself is the use of such information to obtain credit, goods, services, money, or property, or to commit a felony or a misdemeanor.[33]

---

28 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 36.

29 2010 cyber crime report, *Norton: Cybercrime strikes 83 percent of Internet users in Malaysia*, 19 October 2010, http://gadgets.emedia.com.my/product.php?id=1205 (accessed June 11, 2011).

30 Ibid, p 8-9.

31 Judith M. Collins, *Preventing Identity Theft in Your Business, How to Protect Your Business, Customers, and Employees* (Canada: John Wiley & Sons Inc, 2005), 8.

32 "Personally sensitive identifying information" means a person's name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, demand deposit account number, savings or checking account number, credit card number, or mother's maiden name—information needed to obtain an original birth certification for a complete identity takeover.

33 Collins, *Preventing Identity Theft in Your Business, How to Protect Your Business, Customers, and Employees*, n. 31 at 8.

Major trends affecting the security issue in banking and financial institutions in emerging/developing countries are:

(1) the increased complexity and coverage of technology;
(2) the expansion of the number of financial institutions utilizing cutting-edge technologies;
(3) the steady increase in the number of cyber users, especially in conducting financial transactions; and
(4) the lack of laws dealing with cyber crimes.[34]

In this situation, point (3) is very dominant because it the cause of increasing security issue in online banking. Thus, it shows how crucial it is to protect consumer in electronic financial transaction.

It is to be noted that over 700 international e-commerce web sites were examined by The International Marketing Supervision Network (IMSN), an organization consisting trade practices law enforcement authorities of 25 countries. The outcome of the research is the following:[35]

1. More than half businesses failed to outline their payment security mechanisms
2. 62% provided no refund or exchange policies
3. 75% had no privacy policy
4. 78% failed to explain how to lodge a complaint
5. 90% failed to advise customers which law is applied in their transactions
6. 25% showed no physical address

The outcome of the above research shows that there is a very high risk for consumer to do transaction in online banking model. Large number of consumers finds it difficult to claim the refund of their money because most of the online banking system has no refund and privacy policy. Furthermore, the most problem is that the bank failed to advice customers which law is applied in their transactions.

34 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 35.

35 Sonny Zulhuda, "E-Commerce and Consumer Protection in Malaysia," http://sonnyzulhuda.wordpress.com/2009/07/17/e-commerce-and-consumer-protection-in-malaysia/ (accessed June 24, 2011).

Therefore, there are two main approaches to protect the consumer from online banking scams via email. There are legal and regulatory (external approach) and consumer behavior (internal approach).

1. Legal and Regulatory (External Approach)

Legal and regulatory approaches play important role to provide consumer protection. According to Sonny Zulhuda, there are two approaches available in protecting online consumers namely:[36]

a. Legislative Approach: By drafting and enacting a comprehensive legislation on consumer protection in the electronic commerce.
b. Self-Regulatory Approach: By drafting a model code or guidelines on e-commerce consumer protection to be adopted by e-commerce entities and consumer associations.

The author here has identified some legal and regulatory approaches in Malaysia which could be applied to protect consumers in the cyberspace.

Protecting Consumer for Email Scams

The number of cyber criminals via email scams should be considered by regulators because the crime *modus operandi* is changing rapidly. Today, 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 regulated personal data for email scam. Thus, this Act has not protected consumer financial data for email scam specifically.

Generally, this Act has some principles which are able to protect consumer's personnel data in cyber space. Disclosure principle said that "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.[37]

36 Ibid.
37 See sec 8(1) Personal Data Protection Act 2010.

Furthermore, this Act apply security principle that provides: "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".[38] In regards to unauthorised access, it is a very important issue in e-mail scam. It can be done after the perpetrator successfully copied all of the victim's personal financial data.

Unfortunately, the victims never recheck whether the e-mail is spam or not. However, 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 allow a perpetrator to do identity theft activity, and then it can facilitate identity crime.

In unauthorised access context, Computer Crimes Act 1997 has regulated the secure access to any program or data held in a computer. Section 5(1) provides that: "A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer." Thus, this section is important in providing protection of consumer financial information which is caused of modification of the contents of any computer.
In this crime model, a black hat hacker (cracker) would be very dangerous because they can penetrate the computer systems of banks and then he/she is not only able to steal customer data but also is able to modify consumer data. Thus, these can be used for criminal activity. Therefore, this Act can be applied to combat computer crime on hacking activities.

However, these Acts should be harmonized with Consumer Protection Act 1999 because it has not been set up specifically on email scam. This Act focused more on consumer protection in traditional transaction. The Consumer Protection Act 1999 just regulates the safety standard in relation to goods relating to the performance, composition, contents, manufacture, processing, design, construction, finish or packaging of the goods.[39] In other words, this legislation is only to provide basic protection for

38 See sec 9(1) Personal Data Protection Act 2010.
39 See sec 19 Consumer Protection Act 1999.

consumers. Furthermore, section 2(2)(g) provides "This Act shall not apply to any trade transactions effected by electronic means unless otherwise prescribed by the Minister."[40]

In electronic transaction context, Digital Signature Act 1997 is also very important in the protection of illegal transaction which could be carried out by perpetrators. 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 conduct electronic transaction by using "user name" and "password" only. Consumer will get confirmation first if any electronic transaction before it is executed.

In digital edge, the Consumer Protection Act 1999 should consider the use of biometrics technology. This technology can assist in authenticating an individual's identity automatically, and has several useful applications within Justice and Law Enforcement[41] 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 in recognizing authorized account holders of online banking. It can be used in an effort to double security when doing online transaction. Security system which uses card, token or password systems is prone to be stolen or counterfeited. Besides, this system is also used to eliminate telecommunication crime, such as terrorism activities.

In Pakistan, Sim card vendors have been given three months to install biometric technology to confirm the identity of customers.[42] By using biometric technology will produce digital prints which it streamlines procedure to check and cross-reference with multiple databases. This 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

40 See sec 2(2)(g) Consumer Protection Act 1999.

41 *Justice and Law Enforcement Biometrics*, http://findbiometrics.com/applications/justicelaw-enforcement/ (accessed February 12, 2013).

42 *Pakistan to introduce biometric controls for SIM card sales*, http://www.planetbiometrics.com/article-details/i/1372/ (accessed February 12, 2013).

provides transaction, data and web security when operating within databases as well as remote access to resources with mobile technology.[43]

Unfortunately, there is no specific legislation that prohibits the spread of unsolicited email by the recipient based on regulations in Malaysia, although Electronic Commercial Act 2006 has regulated the legal recognition of electronic message.[44] In this regards, Singaporean law has regulated specifically email spam under the Spam Control Act 2007. Basically, the Act contains the framework for regulating unauthorized electronic messages which are regarded as commercial electronic messages for the purposes of the Act, sent by the traditional method of electronic mail ('e-mail'), text and multimedia messaging to mobile telephone numbers.

Protecting Consumer for Typosquatting

Typosquatting is fraud activity which aims to identity theft through phishing. To combat typosquatting infringement, there is no specific regulation in Malaysia. The identity theft activity by using typosquatting strategy is contrary with the business ethics principle. The basic principle of good faith can be applied in this case. It is a universal principle which is generally able to be applied in the tradition of common law system countries.

This infringement is much related to registered trademark infringement. Registration domain name is made in their respective countries. In Malaysia, domain name can be registered under My Domain Register (MYNIC) at www.mynic.net. In this case, MYNIC should filter domain name which will register whether the suspect infringes trademark protection principle or not. For example, there is a domain name dispute on case of 'www.ocbc.my'. The first complainant, Oversea-Chinese Banking Corporation Limited, is a prominent commercial bank incorporated in Singapore which has been operating for many years in Singapore and Malaysia. The second complainant, OCBC Bank (Malaysia) Berhad is the Malaysian subsidiary of the first complainant and the registered

43 *Justice and Law Enforcement Biometrics*, n. 41.
44 See sec 6, Electronic Commercial Act 2006.

proprietor of the website 'www.ocbc.com.my', which it uses to promote its business.[45]

In the above case, the panel decided in favor of the complainants on two grounds: namely, that the disputed domain name was confusingly similar to the OCBC mark and that it was registered in bad faith. The respondent was ordered to transfer the disputed domain name to the second complainant. The respondent knew that he was appropriating a well-known name in view of the reputation and prominence of the OCBC mark in Malaysia and other countries. Thus, the panel held that the respondent had registered the disputed domain name in bad faith.[46] Furthermore, in this case the principle of good faith can be applied because the perpetrator registered a domain name very similar with a well known trademark. Thus, it creates confusion on the part of the consumers to access the legal website. In this regards, crime perpetrators create a nearly identical site to the site of potential victims. Therefore, the typosquatter will register fake domain names to enforce typographical errors by consumers. It weakens the fundamental trademark principle of consumer protection by permitting ruthless competitors to benefit from the mark holder's good will and reputation.[47] It is easy for typosquatters to register the trademark and then connect to "phishing site".

In this regards, Malaysian Communications and Multimedia Commission (MCMC) has important role to control phishing activities. MCMC has a responsibility to regulate communications and multimedia industry. Thus, MCMC can block the suspected illegal websites or violate copyright website. In 2011, MCMC has blocked 10 such website[48] in Malaysia.

Protecting Consumers from Phishing Scams

In fact, identity theft scams via email relates to "phishing scam". It is one of the trends in cyber crimes. The email sent would appear

45 Soo, Michael, Lee Lin Li and Olivia Khor Shook Lin & Bok, *Malaysia: New case law shakes up thinking on trademarks,* Building and enforcing intellectual property value 2011, pp 168-169.

46 Ibid.

47 Gilwit, *The Latest Cybersquatting Trend*, 9.

48 M. Kumar, Wong Pek Mei and Jo Timbuong, "No more free downloads as MCMC blocks 10 files sharing sites," *The Star Newspaper*, Saturday (accessed June 11, 2011).

as if it came 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. In this case, consumers will unsuspectingly automatically "clicked on" the link provided to fake banking website. In this situation, it is hard for the victims to distinguish the fake website and original one.

In this regards, MCMC has an important role to play in controlling cyber activities. By forming Cyber Security Malaysia (CSM), control for phishing site is more effective. Currently, 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.[49] In fact scams targeting electronic banking have increased dramatically in the country with the number more than doubling over the past years. A total of 1,426 reports were made to CSM[50] last year compared with 634 in 2009.[51]

Phishing Scams will facilitate computer crime through identity theft. The increase of computer crimes must be a significant concern for any law enforcement agency or for anyone responsible for security on any network.[52] This is done in an effort to suppress small as possible victims of crimes committed by perpetrators of fraud through email scams. Imagine, more than 4,000 cyber complaints, mostly concerning cyber crimes have been lodged with CSM in the past two years.[53] How vulnerable consumer's identity data is.

---

49 *E-banking scams on the rise,* Wednesday February 16, 2011, *The Star Newspaper*, http://www.thestar.com.my/news/story.asp?sec=nation&file=/2011/2/16/nation/8071653 (accessed June 8, 2011).

50 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 June 8, 2011).

51 *E-banking scams on the rise*, n. 49.

52 *E-banking scams on the rise*, n. 49 at 3.

53 *More than 4,000 cybercrime cases reported in Malaysia within two years,* http://sanooaung.wordpress.com/2009/01/17/more-than-4000-cybercrime-cases-reported-in-malaysia-within-two-years (accessed June 10, 2011).

Therefore, the Malaysian government has a responsibility to give real power to cyber security decision-makers, and alert its citizens and civil servants of the dangers of cyber crime by forming CSM, which reports to the Ministry of Science, Technology & Innovation (MOSTI).[54] Furthermore, it is also an effective way to protect consumers in electronic transaction by contacting Cyber 999 Help Centre.

Existence of CSM is very important to protect consumer from cyber crime activities. The public can report hack attempts, malicious codes, denial-of-service attacks and intrusion via CSM's website. Cyber 999 is a public service that provides emergency response to computer security related emergencies as well as assistance in handling incidents such as computer abuses, hack attempts and other information security breaches.[55] This team is able to provide law enforcement for protecting consumers in cyber activities.

It is important to note that it is meaningless to have plethora of legislation without making internal banking regulation a priority. Therefore, it is very important that all banking and financial services in Malaysia be regulated by its Central Bank, Bank Negara Malaysia (BNM). Internet banking was introduced in Malaysia in June 2000 when BNM allowed the local banks to offer Internet banking services in Malaysia. BNM has provided Minimum Guidelines on the Provision of Internet Banking Services by Licensed Banking Institutions (MGIB) 2000 modeled.[56]

The aim of the MGIB is to protect both consumers and the banks themselves from the risks associated with such banking.[57]

---

54 "*Malaysia Vs Malware*", Futures Magazine - Issue 5.1 http://www.cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1900/index.html (access June 10, 2011).

55 *Cybersecurity Malaysia Intensifies Fight Against Cybercrime,* Wednesday, 27 April 201, http://www.malaysiandigest.com/news/21919-cybersecurity-malaysia-intensifies-fight-against-cybercrime.html (access June 10, 2011).

56 BNM defines Internet banking as being 'products and services offered by licensed banking institutions on the internet through access devices, including personal computers and other intelligent devices'. Banking institutions are legal entities licensed under the Banking and Financial Institutions Act (BAFIA) 1989.

57 Gita Radhakrishna, "Liability Issues in Internet Banking In Malaysia," *Communications of the IBIMA* 7, (2009): 1

C. Consumer Behavior (Internal Approach).

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. All of these investments can serve an important role in safeguarding today's highly IT-dependent financial institutions but, by themselves, they are insufficient. However, over reliance 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.[58] Therefore, it is important to combat online banking scams through consumer behavior approach. Online banks should have internal regulatory and security system, such as adding mechanisms whereby consumers can verify that they are visiting the real site. In this situation, banks and consumers need improve their interaction for the sake of protecting consumers in cyber activity.

In this regards, it is very important for banks to provide training and equipping their consumers as BNM required. Banks need to educate customers on their role in maintaining security of banking information and remind consumers of the risks involved in using online banking. Thus, prior to the offering of Internet banking services, BNM requires banks to have a web page to educate their customers on the various issues such as knowledge of the risks involved in using the Internet banking, e.g. risk of 'phishing', advised to read the privacy policy statements prior to providing any personal information to any third party advertisers or hyper text web links, and educating customers on their role in maintaining security of banking information.

In this situation, consumer behavior approach is very important for controlling their emotion when getting "surprising email". Bank should train the consumers not to follow links that have been e-mailed to them before checking the real website. If you receive an e-mail purporting to be from a financial institution, then either

58 Shalhoub and Al Qasimi, *Cyber Law and Cyber Security in Developing and Emerging Economies*, n. 13 at 35.

call the organization or manually enter the URL you normally use to access your account. Phishing site is professionally designed and difficult to identify, especially for beginners in online banking transaction. Therefore, it is very important to avoid clicking on any links provided in the e-mails.

Furthermore, consumers should contact the bank or retailer by phone to verify if the e-mail was genuine because there is no anti-virus that can give us 100 % protection for email scams. Therefore, the most effective protection is to develop the consumer right habit. Consumers need to learn and practice these safe surfing habits.

Conclusion

In general, this paper identified that cyber scams activities via email in online banking business model are email scams, typosquatting and phishing scams. These scams model will begin from unsolicited email which informs a misleading news of website addresses which is using typosquatting strategy in order to link with the fake website. It is certain that the fake website contained much well-known trademark infringement. However, the goal is to obtain personal financial information. In this regards, Malaysian laws have regulated consumer protection for commercial activities via various means i.e. traditionally and electronically. However, there is no specific regulation on controlling email scams. Thus, development of future legislation of consumer protection should consider making regulation for email spam control. Furthermore, there is also a need to consider the use of biometrics technology for assisting in authenticating an individual's identity automatically. This technology can also assist in recognizing the authorized account holder while using online banking transaction.

All in all, in this paper the author also addressed that consumer protection of online banking scams in Malaysia could be viewed from two perspectives or approaches. These two approaches are legal and regulatory (external approach) and consumer behavior (internal approach). These approaches are interconnected to each other in the protection of consumers. In this regards, protecting consumers through written regulation is insufficient. Thus, it is very important for banks to provide training and equipping consumers with enough

information as BNM required. In this case, role of FMB and Cyber 999 Help Centre to assist consumer to investigate the crime and to assist refund is very important.

Bibliography

Collins, M. Judith. *Preventing Identity Theft in Your Business, How to Protect Your, Business, Customers, and Employees*. Canada: John Wiley & Sons Inc, 2005.

Cybersecurity Malaysia Intensifies Fight Against Cybercrime, Wednesday, 27 April 201, http://www.malaysiandigest.com/news/21919-cybersecurity-malaysia-intensifies-fight-against-cybercrime.html (accessed June 10, 2011).

Dara B. Gilwit, *The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How To Prevent Public Deception and Trademark Infringement*, http://law.wustl.edu/Journal/11/p267Gilwitnotebookpages.pdf, p.6 (accessed July 12, 2011).

Easttom, Chuck and Taylor, Jeff. *Computer Crime, Investigation, and the Law*. USA: Course Technology Cengage Learning PTR, 2011.

"E-banking scams on the rise." Wednesday February 16, 2011, *The Star Newspaper*,

E-commerce in Malaysia, http://www.getranked.com.my/e-commerce/e-commerce-in-malaysia.html (accessed October 20, 2012).

How to Report Fraud and Scams, http://www.419legal.org/blog/2010/04/12/how-to-report-fraud-and-scams/ (accessed February 22, 2011).

Justice and Law Enforcement Biometrics, http://findbiometrics.com/applications/justicelaw-enforcement/ (accessed February 12, 2013).

L, Bielski. "Phishing phace- of: Online fraudsters and vendors do battle to gain control of electronic information." *ABA Banking Journal* 96, no. 9 (September 2004): 46-54.

M. Kumar, Wong Pek Mei and Jo Timbuong. "No more free downloads as MCMC blocks 10 files sharing sites." *The Star Newspaper*, Saturday (accessed June 11, 2011).

Malaysia Experiencing Rise in Cyber Crimes, http://www.spamfighter.com/News-11776-Malaysia-Experiencing-Rise-in-Cyber-Crimes.htm (accessed June 11, 2011).

"*Malaysia Vs Malware*", *Futures Magazine - Issue 5.1* http://www.cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1900/index.html (accessed June 10, 2011).

More than 4,000 cybercrime cases reported in Malaysia within two years, http://sanooaung.wordpress.com/2009/01/17/more-than-4000-cybercrime-cases-reported-in-malaysia-within-two-years (accessed June 10, 2011).

P. Aruna. "Don't fall prey to online banking scams." *The Star Newspaper*, Saturday February 19, 2011, http://thestar.com.my/news/story.asp?file=/2011/2/19/nation/8039959&sec=nation (accessed June 5, 2011).

P. Aruna, "Rise in scams targeting e-banking accounts." *The Star Newspaper*, Wednesday February 16, 2011, http://thestar.com.my/news/story.asp?file=/2011/2/16/nation/8073924&sec=nation (accessed June 5, 2011).

Pakistan to introduce biometric controls for SIM card sales, http://www.planetbiometrics.com/article-details/i/1372/ (accessed February 12, 2013).

Radhakrishna, Gita. "Liability Issues in Internet Banking In Malaysia." *Communications of the IBIMA* 7, (2009): 1-15.

Seah, Tommy. "Cyber Crime Tops List of Most Common Crimes in Malaysia, Cyber Crime Cyber Security Malaysia." http://www.thenewnewinternet.com/2010/04/15/cyber-crime-tops-list-of-most-common-crimes-in-malaysia/ (accessed June 11, 2011).

Sonny Zulhuda. "E-Commerce and Consumer Protection in Malaysia." http://sonnyzulhuda.wordpress.com/2009/07/17/e-commerce-and-consumer-protection-in-malaysia/ (accessed June 24, 2011).

Soo, Michael, Lee Lin Li and Olivia Khor Shook Lin & Bok, *Malaysia: New case law shakes up thinking on trademarks,* Building and enforcing intellectual property value 2011, pp.168-169.

The 2010 cyber crime report, *Norton: Cybercrime strikes 83 percent of Internet users in Malaysia*, 19 October 2010, http://gadgets.emedia.com.my/product.php?id=1205 (accessed June 11, 2011).

What Are Identity Theft and Identity Fraud? http://www.justice.gov/criminal/fraud/websites/idtheft.html (accessed May 10, 2013).

What Is a Phishing Scam?,http://www.wisegeek.com/what-is-a-phishing-scam.htm (accessed June 5, 2011).

Zeinab Karake Shalhoub, and Sheikha Lubna Al Qasimi. *Cyber Law and Cyber Security in Developing and Emerging Economies.* USA: Edward Elgar Publishing, 2010.

Statutes

Banking and Financial Institutions Act (BAFIA) 1989.
Computer Crimes Act 1997 (Act 563)
Consumer Protection Act 1999 (Act 599)
Digital Signature Act 1997 (Act 562)
E-commerce Act 2006
Electronic Commercial Act 2006
Malaysian Communications and Multimedia Commission Act 1998 (Act 589)
Communications and Multimedia Act 1998 (Act 588)
Personal Data Protection Act 2010 (Act 709)
Singapore Spam Control Act 2007