Islamic Law Perspective on Cybercrime in The Financial Services Industry

1st JM Muslimin, 2nd Siti Ida Farida, 3rd Maulidia Permata Citra, 4th Mu'min Roup[4]
{jm.muslimin@uinjkt.ac.id[1], sitiidafarida21@mhs.uinjkt.ac.id[2],
maulidiapermatacitra21@mhs.uinjkt.ac.id[3], muminrauf@uinjkt.ac.id[4]}

UIN Syarif Hidayatullah Jakarta[1,2,3,4]

Abstract. *Cybercrime* is a crime today that is not limited by time, place, and region and causes harm. Crimes are committed only through computers so that these crimes are difficult to identify. The method used in this study is a normative juridical approach, by reviewing, testing, and examining legal aspects, especially criminal law related to cybercrimes by researching secondary data in the field of law, namely; types of data obtained from library research (library research), and other data related to the title of this research. The purpose of this study is to determine the review of Islamic law in Indonesia against crime *cyber*crime in the banking world caused by the lack of information obtained by customers regarding the security of a system, the lack of education related to the modes that often occur in the world of digital banking such as *phishing*, *sniffing*, *pharming*, etc.

Keywords: *Cyber Crime*, Islamic Law, Internet Banking and Mobile Banking

1 Introduction

The use of internet media today can not be separated in everyday life. One of them is in the financial services industry such as banks that issue internet banking and mobile banking services to make it easier for customers to transfer funds, balance information, account mutations, exchange rate information, payments (credit cards, electricity bills, telephone accounts, insurance), and purchases. (top-up credit, shares).

Digital banking services have experienced accelerated growth since the Covid-19 pandemic. both in terms of the level of technology used and in its operational activities. The function of information technology itself, in general, is to improve the efficiency and effectiveness of banking operations to increase the contribution of banks in improving the national economy, following the function of the formation of a bank, namely as an agent of development, agent of trust, and agent of equality. In addition, the existence of banks in Indonesia is also highly expected to become good corporate governance in the national banking industry. In Bank Indonesia regulations, Bank Indonesia urges all banks in Indonesia to take advantage of Internet media in the form of a homepage or website that they own and manage, and requires transparency of their financial statements on the Internet as an effort to increase public trust in the existence and existence of a bank.

The presence of internet banking and mobile banking makes banking transactions more practical, easy, and fast. The increasingly modern era makes everything digital, it can even be said that direct transaction activities at the Bank are very rare. Whereas ten years ago, banking

ICIIS and ICESTIIS 2021, October 20-21, Jambi, Indonesia

DOI 10.4108/eai.20-10-2021.2316344

transactions were still carried out manually even though they had to work long distances and queues.

Thanks to technological advances, online banking transaction methods or commonly referred to as internet banking and mobile banking have become the people's choice today. Customers can easily perform banking transactions anytime and anywhere just by preparing electronic devices such as smartphones (smartphones), computers, laptops, and the like that are connected to the internet network. However, the convenience that we get today must be accompanied by awareness and prudent personal data so that transactions always run safely. This is because digital banking services can be accessed more easily than physical banking services, which require an ATM card and passbook. Crimes in electronic transactions are carried out by someone who has expertise in using the system or what is often called (Cyber Crime).

Cybercrimes often occur in the banking world. The reasons are various, but mainly because customers do not know, are negligent, underestimate, or even lazy to seek information on how to transact securely. However, cybercrime in the banking sector needs to be dealt with seriously because this crime is not only detrimental to customers and banks but can also damage the world economic system. The phenomenon of cybercrime in the banking sector has its characteristics compared to crimes in general because in this crime there is no definite target victim so that anyone can become a victim of this crime. So every user of internet services must also be very wary of this crime. This crime is global which allows cybercrime to be carried out without recognizing territorial boundaries and does not require direct interaction between the perpetrator and the victim of the crime.

2 Methodology

This research is normative juridical research where the author only examines the rule of law based on the facts that occur related to the regulation of information and electronic transactions, especially in the field of financial services. The data used are secondary, obtained from various books, journals, and news which is then identified.

3 Result and Discussion

3.1 Definition of Cyber Crime

Before describing the definition of cybercrime in detail, it will first be explained the "mother" of cybercrime, namely cyberspace. Cyberspace is seen as a world of computer-based communication. In its working system, cyberspace (internet) changes to distance and time to be unlimited [1]. Abuse in cyberspace is known as cybercrime. *Cybercrime* is a crime using information technology and is a form of transnational crime that knows no boundaries (borderless), without violence (non-violence), no physical contact (no physical contact) and without a name, so that the perpetrators of Cyber Crime very difficult to trace and the criminal elements are difficult to prove [2].

Cybercrime is one of the new forms of today's crime that has received wide attention, both nationally, regionally, and internationally [3]. Volodymyr Golubev called it "the new form of anti-social behavior". Several other "pretty cool" nicknames were given to this new type of

crime, including: "cyberspace/virtual space offense", a new dimension of "Hitech crime", a new dimension of "transnational crime", and a new dimension of “white-collar crime” [4].

The rapid development of cybercrime can be seen from the emergence of various terms, such as economic cybercrime, EFT (Electronic Fund Transfer) crime, cyberbank crime, Internet banking crime, online Business Crime, Cyber/Electronic Money laundering, Hitech WCC (White Collar Crime), Internet Fraud, Cyber Terrorism, Cyber Stalking, Cyber Sex, Cyber Chile Pornography, Cyber Defamation, Cyber Criminals, etc [5].

Cyber Crime or "CC" can be divided into two categories, namely "CC in a narrow sense" ("in a narrow sense") called "computer crime" and "CC in a broad sense" called "Computer-Related Crime” (CRC) [6].

1. *Cybercrime* (CC) in a narrow sense (*Computer Crime*): *any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them*.
2. *CC in a broader sense (Computer-Related Crime): any illegal behavior committed by means of, or in relation to a computer system or network, including such crimes as illegal possession, offering, or distributing information by means of a computer system or network.*

In the first category, CC includes crimes committed: (1) by means of a computer system or network ("by means of a computer system or network"); (2) in a computer system/network (“in a computer system or network”);. Meanwhile, in the second category, CC includes crimes committed against computer systems/networks (“against a computer system or network”) [7].

3.2 Cyber Crime Mode in the Financial Services Sector

Banking crime was born and grew along with the progress of science and technology achieved by humans. These crimes are included in the category of "elite" class crimes. Said to be "elite", because not everyone can do it. This "elite" class crime does not require a lot of physical strength. Thinking ability is an important factor to achieve multiple results. The more advanced and developing human civilization, the more colors and forms of evil will appear to the surface. Therefore, after computers are rampant in various parts of the world, people are then busy and bothered with the side effects it causes, namely in the form of computer crime (cybercrime). When we talk about high-tech crimes such as Internet crimes or cybercrime, it is as if the law is behind the scenes (het recht hink achter de feiten aan). Along with the development of the use of the Internet, those who have the ability in the field of computers and have certain purposes can use computers and the Internet to commit crimes or "mischief" that harms other parties.

Cybercrimes in the financial services sector are generally divided into two types, namely social engineering and skimming. Social engineering is the crime of psychologically manipulating someone to get certain information or to do certain things using subtly deceiving, which is done via telephone or direct talk. Meanwhile, skimming is the act of stealing information by illegally copying the information contained on the magnetic stripe of a debit or credit card or using a data recording device on an ATM/ electronic data capture (EDC) machine [8].

The basic techniques of obtaining information with various social engineering modes include:

a. *Phishing*, namely the act of illegally obtaining personal information such as user ID, PIN, bank account number/credit card number. This information is then used to access accounts, commit credit card fraud, or guide customers to make transfers to certain accounts with the lure of prizes or to transact on behalf of the customer. Perpetrator*phishing* usually targets the last 4 digits on the credit card and pin. There is

a common technique where credit card data theft is often carried out, namely the perpetrator calls and claims to be a representative of the bank who wants to update credit card data. Another mode that is often used is to create fake online shopping sites [9].

b. *Keylogger*/*keystroke logger*, Software on a computer like this can record every keyboard key that is used without the user realizing it. And it often happens in public Internet access places such as in internet cafes [10]. The more often you access the Internet in public places, the more vulnerable you are to being trapped by this type of modus operandi because many users use the computer interchangeably.
c. *Sniffing* is the method used by the perpetrator by observing the internet data package used by the user to obtain the identification number and password in question [11].
d. *Pharming*fraudsters or hackers redirect from legitimate sites to fake sites without the victim knowing and realizing it. Then take the data entered by the victim so that it enters the area that is the game of the fraudster.
e. *Spoofing*use software to mask identity by displaying a fake e-mail address/name/phone number on a computer to hide identity. To commit fraud they give the impression of dealing with reputable businessmen.
f. Typo site, which makes the domain name and site address similar to the official site. Perpetrators take advantage of mistakes from internet users in typing the address of the site they are looking for.
g. Brute Force Attacking, which is an attempt to steal identity numbers and passwords by trying the possible combinations made
h. Web Deface : System Exploitation, namely exploiting the system by changing the initial appearance of an official website.
i. Email Spamming, namely by sending an email to the account owner by offering products or stating that the account owner has won a sweepstake.
j. Denial of Service, namely the disabling of electronic systems by flooding accounts or electronic systems with large amounts of data.
k. Viruses, worms, trojans: The spread of computer viruses is carried out to attack computer systems, obtain data, manipulate data or other actions carried out against the law.

3.3 Positive Legal Perspectives and Islamic Law on Digital Crime

Cybercrime in the financial services sector is very impactful for its existence because it can affect the level of customer trust (reputation risk) [12]. So that efforts are needed to prevent and take action against cybercrime perpetrators in financial services. The legal basis for determining sanctions for perpetrators is cybercrime, namely: First, cybercrime can be categorized as one of the modes of fraud as the word of Allah SWT contained in QS Asy-Syu'ara' verse 183 and Al-Maidah: 38.

وَلَا تَبْخَسُوا النَّاسَ أَشْيَاءَهُمْ وَلَا تَعْثَوْا فِي الْأَرْضِ مُفْسِدِينَ

Meaning: "And do not harm people by reducing their rights and do not make mischief on the earth." (Surah Asy-Syu'ara': 183).

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالًا مِنَ اللَّهِ ۗ وَاللَّهُ عَزِيزٌ حَكِيمٌ

Meaning: "Men who steal and women who steal, cut off their hands (as) retribution for what they do and as a punishment from Allah. and Allah is Mighty, Wise." (Surah Al-Maidah: 38).

From the second sense. The Qur'anic verse above explains that the prohibition for a Muslim to do activities that can harm others and damage the peace in the world and the sanctions given to anyone who commits theft then the punishment is following that described in QS Al-Maidah verse 38, Second In a The hadith narrated by Ibn Hibban regarding cheating is that the Prophet SAW said:

مَنْ غَشَّنَا فَلَيْسَ مِنَّا، وَالْمَكْرُ وَالْخِدَاعُ فِي النَّارِ

Meaning: "Whoever cheats, then he is not from our group. People who commit treason and deception, his place in hell "(HR. Ibn Hibban 2: 326. This hadith is authentic as said Shaykh Al Albani in Ash Shahihah no. 1058) [13].

In addition, there is also a Hadith of the Prophet narrated by Imam Ibn Majah, al-Daraquthni, and others, from Abu Sa'id al-Khudri, the Prophet said:

لَا ضَرَرَ وَلَا ضِرَارَ

Meaning: "You must not harm (harm) yourself or others."

The problem of cybercrime cannot be included in the jarimah hudud category because the form of the crime is not measurable (abstract). However, the problem regarding cybercrime is more precisely in the jarimah category with ta'zir criminal sanctions applied to criminals who commit violations both related to God's rights and human rights and are contemporary problems that occur due to the times.

Punishment for perpetrators of cybercrime will be delegated to ulil amri who will then be considered in accordance with the elements of the crime committed by the perpetrator so that the punishment prescribed can be educational (ta'dîb) in the sense of anticipating by means of frightening (tankîf) [14].

In Indonesia, all forms of information crime and electronic transactions are regulated in Law No. 11 of 2008 concerning Electronic Information and Transactions which was later changed to Law No. 19 of 2016, which regulations regarding data falsification have been contained in chapters 30, 31, 32, 46, 47, and 48 which reads:[15]

Chapter 30:

Any Person intentionally and without rights or against the law accessing a computer and/or electronic system in the way by violating, breaking through, exceeding, or breaking into the security system, to obtain Electronic Information and/or Electronic Documents.

Chapter 31:

Every Person intentionally and without rights or against the law conducts wiretapping, interception of the transmission of Electronic Information and/or Electronic Documents that are not public from, to, and within a certain Computer and/or Electronic System belonging to another person, both of which do not cause any changes or those that cause changes, omissions, and/or termination of Electronic Information and/or Electronic Documents that are being transmitted.

Chapter 32:

Any person intentionally and without rights or against the law in any way alters, adds, reduces, transmits, destroys, removes, transfers, hides an Electronic Information and/or Electronic Document belonging to another person or the public or transferring/transferring Electronic Information and/or Electronic Documents to the Electronic Systems of other unauthorized persons.

Chapter 46:
Everyone who fulfills the elements as referred to in

1. Chapter 30 paragraph (1) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp.600,000,000.00 (six hundred million rupiahs).
2. Chapter 30 paragraph (2) shall be sentenced to a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiahs).
3. Chapter 30 paragraph shall be sentenced to a maximum imprisonment of eight years and/or a maximum fine of Rp. 800.000.000,- (Eight Hundred Million Rupiah).

Chapter 47:

1) Everyone who fulfills the elements as referred to in chapter 31 paragraph (1) or paragraph (2) shall be sentenced to a maximum imprisonment of ten years and/or a maximum fine of Rp 800.000.000,- (Eight Hundred Million Rupiah).

Chapter 48:
Everyone who fulfills the elements as referred to in:

1. Chapter 32 paragraph (1) shall be sentenced to a maximum imprisonment of 8 years and/or a maximum fine of Rp. 2.000.000.000,- (Two Billion Rupiah).
2. Chapter 32 paragraph (2) shall be sentenced to a maximum imprisonment of 9 (nine) years and/or a maximum fine of Rp. 3.000.000.000,- (Three Billion Rupiah).
3. Chapter 32 paragraph (3) shall be sentenced to a maximum imprisonment of ten years and/or a maximum fine of Rp. 5.000.000.000,- (Five Billion Rupiah).

The presence of the ITE Law is a response to violations and crimes in the field of technology and information that are increasingly happening today. However, it can be seen that the points contained are only limited to the rules that ensnare and punish people who commit cybercrimes. The ITE Law should also be able to provide answers to who should be responsible for the losses that befall customers due to cybercrime. If the bank does not want to be responsible, then how is customer protection? The emergence of banking crime (cybercrime) must also be supported by adequate regulations, whether issued by relevant regulatory bodies such as Bank Indonesia or by agencies such as self-regulatory bodies. So far, the government has not considered IT crimes as a top priority in law enforcement policies compared to handling terrorism, treason, and separatist movements in several regions.

Several efforts to prevent criminal acts, or to handle criminal acts where the ITE Law is the legal basis in the law enforcement process against crimes using electronic and computer (cybercrime) facilities, include:

1. limitation or limitation of responsibility so that the responsibility of the organizer does not exceed reasonableness.
2. Second, all electronic information and electronic signatures produced by an information system, including the printouts, must be able to become evidence in court.
3. Third, the need for legal protection for the Central Bank, and banking/financial institutions, credit card/payment card issuers, and other financial institutions from the possibility of interference and threats of electronic crime. In this ITE Law, such protection can be carried out by criminalizing any illegal use and access to the computer of the institution/institution, given the very vital role of financial institutions in the economy and to maintain the level of public trust in financial institutions.
4. Fourth, the need for deterrent criminal threats against electronic crimes (Cybercrime), so that they can protect the integrity of the system and the investment value that has been built with a fairly large allocation of resources.

For banks themselves, efforts to prevent technology fraud or cybercrime can be carried out through improving the bank's operational procedure system and periodically checking or

reviewing the capacity and adequacy of banking risk control or risk control as an early warning system. This is done as part of the oversight supervision carried out on the bank. Although preventive measures must be taken, no less important is the guarantee of legal protection for customers from the possibility of technology fraud or cybercrime.

Specifically, in the context of law enforcement and prevention of banking crimes, the steps that must be taken are:

1. The need to increase the ability of investigators in the accounting and finance fields;
2. The supervisory system from the bank is effective and this can be done if the recruitment of employees places more emphasis on mental ideology;
3. The need for the investigator's authority in carrying out his duties, not only regarding bank secrecy;
4. The need for reform of legislation in the economic field, in case banking laws.

The tips for safe transactions using internet banking include:

1. Type the Bank URL Correctly, Make Sure There is a Padlock Sign Internet banking crimes often stem from the existence of a fake website that resembles the bank's original website. There is also a login button on the fake website, which if you log in, your data will become theirs. Therefore, make sure you check and type in the official bank URL correctly. Ignore if there is an incoming email in the name of the bank and asks you to click or send personal data.
2. Don't Share PIN/Password/OTP Code Know that in online banking transactions, data such as usernames, PINs, passwords, and even OTP codes for internet banking access are important. Not only that, other data such as account numbers, credit card numbers, CVV (3 digit numbers on the back of the card), OTP code, and credit/debit card expiration dates are also important Never share your banking data with others. In addition, never give/share your selfie photo by holding your identity (KTP/NPWP) because this is also prone to fraud.
3. Diligently Update/Change Password/PIN Change internet banking password/PIN periodically at least every 6 months.
4. Make sure the log out is complete with the transaction after completing the transaction, you must press the log out button on the website. Although it looks trivial, this is important to note, because negligence like this can make your bank account controlled by irresponsible people and you will lose.
5. Diligently Clean Internet History on Mobile/Laptop cache and Cookies on your device can be used by Crackers to gain access to your account. Therefore, it is highly recommended to always clear Cache and Cookies after or before making online banking transactions for the security of your data and money.
6. Avoid Random Downloads of Software/Applications be aware of new software and applications when downloading. Sometimes when downloading a movie, song, or application, there will be several applications that are automatically installed on your device which may be the application/software that can record all kinds of your activities online including when you log in for internet banking.
7. Avoid Transactions using Public WIFI, Free VPN, or People's Cell Phones Avoid internet banking transactions using public Wifi connections such as in cafes or using free VPNs because many modes of phishing scams start from public wifi and free VPNs.
8. Don't be easily tempted one of the keys not to being deceived is not to be easily tempted. The saying goes 'There is no free lunch so you should always be careful.

Never be tempted by the seduction of parties who distribute millions of rupiah prizes for free because it is a fraud that has been planned to steal your money.

9. Routinely Check Accounts routine checking of accounts needs to be done. So that if there is a suspicious transaction, it can immediately report it to the bank so that the account can be blocked.

4 Conclusion

In Islamic economic law, in addition to prioritizing contracts, pillars, and conditions in carrying out muamalah, it is also necessary to avoid injustice in gaining profits because acts of injustice can cause injustice to other parties. In addition, we also need to know how Islam views halal or haram income obtained based on objects or processes for profit.

In Islamic Economics, goods that are forbidden are classified into 2, namely: first, haram because of the substance and the second which is forbidden not because of the substance, but because of the way to obtain it by means of the forbidden, for example, stealing, robbing, cheating, etc. Cybercrime mode in banking services such as phishing, spoofing, keylogger, Pharming, Sniffing, is a fraudulent crime mode that is carried out through the internet and is detrimental.

Based on Islamic law that a thief can be given sanctions following what has been described according to QS al-maidah verse 38, but because our country is based on law, sanctions can be given by the law on electronic information and transactions.

References

[1] Maskun. Kejahatan Siber. Jakarta:Kencana. Prenada Media Group. 2013.

[2] Thantawi, dkk. *Perlindungan Korban Tindak Pidana Cyber Crime Dalam Sistem Hukum Pidana Indonesia*. Jurnal Ilmu Hukum. Volume 2. No.1. Februari 2014 Ahmad W arson Munawwir. Kamus al Munawwir. Yogyakarta: Pesantren Krafyak. 1984.

[3] Didik M. Arief Mansur dan Elisatris Gultom, *Cyber Law*: Aspek Hukum Teknologi Informasi. Refka Aditama. Bandung. 2005**.**

[4] Barda Nawawi Arief. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia. Jakarta: Raja Grafindo Persada. 2006.

[5] "Background paper" Kongres PBB X untuk "*Workshop on crimes related to the computer network*". dokumen A/CONF.187/10, 3-2-2000. dalam Barda Nawawi Arief. 2006.

[6] Dwi Haryadi. Kebijakan Integritar Penanggulangan Cyberporn di Indonesia.

[7] Nunuk Sulisrudatin. Analisa Kasus Cyber Crime Bidang Perbankan Brupa Modus Pencurian Data Kartu Kredit. Jurnal Ilmiah Hukum Dirgantara–Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma. Vol 9 No. 1. September 2018.

[8] Abdurrakhman Alhakim & Sovia. Kajian Normatif Penanganan *Cyber Crime* Di Sektor Perbankan Di Indonesia. E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha. Vol 4. No 2. 2021.

[9] Ali Fuad Hasyim. Implementasi Perlindungan Korban *Cyber Crime* Dalam Bidang Perbankan Dalam Peraturan Hukum Pidana Indonesia. Artikel Hukum.

[10] Tri Kuncoro, Penegakan Hukum Terhadap Cyber Crime Di Bidang Perbankan Sebagai Kejahatan Transnasional, Jurnal Megister Hukum Udayana Vol 2 No. 3. 2013.

[11] Nida Rafa Arofah & Yeni Priatnasari. *Jurnal Pendidikan Akuntansi Indonesia.* Vol. 18. No. 2. 2020.

[12] Muhammad Abduh Tuasikal. "Hukum Menjual Produk Imitasi/KW". https://rumaysho.com/10343-hukum-menjual-produk-imitasi-kw.html

[13] Suharyadi, dkk. *Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam*. Journal of Lex Generalis (JLS). Volume. No. 5. Oktober 2020.
[14] Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
[15] Al-Quran -Al Karim.