www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Law Enforcement against Cybercrime in Banking in the Form of Theft of Customer Data

Bintara Sura Priambada[1], Ashinta Sekar Bidari[2], Elisa Putri Oktaviani[3]
[1,2,3]*Universitas Surakarta, Indonesia*
bintara.sp@gmail.com, ashintsb.lawfaculty@gmail.com, elisa.okt08@gmail.com

Abstract

Cybercrime has various types, one of which is phishing. A phishing attack is a cybercrime in which users are tricked into sharing their personal data, such as credit card details, teller machines card details, passwords, and giving hackers access to their device, often without realizing it. Basically phishing is an infection that attacks a computer, cellphone or other device by tricking someone into downloading it. The type of research used is empirical legal research. The technique used is interview technique and document study. Analysis of the data used is qualitative data analysis. The results of the study indicate that Indonesia itself already has laws and regulations relating to electronic transactions ranging from the running of electronic transactions to the regulation of crimes, especially those related to banking such as phishing. The sentencing process for the perpetrators is intended to provide a deterrent effect and ensure the entire security of internet banking application users contained in the terms and conditions section which contains the rights and obligations of customers and banks.

Keywords
cybercrime; banking; phishing

I. Introduction

Globalization is a situation where all walks of life in the world can freely exchange information without any restrictions. All information good or bad can be easily sent and obtained quickly and easily using the Internet. The development of science and technology in addition to having a negative impact also has a positive impact, one of which is the emergence of the internet. Currently, the internet has become a basic and important need to facilitate human work in obtaining information sharing. The impact of the development of information technology is a change in social behavior in human civilization globally. The current of globalization that currently makes distance is not a problem anymore. Humans are getting easier to relate and make transactions with other humans. In addition, it raises the latest innovations in the world of trade.

In recent years, online commerce or what is often known as e-commerce is growing in Indonesia. The community is increasingly facilitated by the existence of e-commerce. Therefore, online buying and selling sites are increasingly popping up. One of the aspects of financial life that is rapidly developing following technology is the use of internet banking. One of these financial facilities has provided various conveniences in both transactions. The banking world is experiencing the impact of technological advances in every transaction. Relationships between humans in the era of globalization are getting easier just by using a smartphone to make buying and selling transactions. Seeing the legal facts as they exist at this time, the impact of the development of science and technology that has been misused as a means of crime is very important to anticipate how the legal policy is, so that cybercrime that occurs can be overcome with criminal law, including in this case regarding proof system.

In the enforcement of criminal law, the basic justification for a person can be said to be guilty or not committing a crime, in addition to his actions being blamed on the strength of the existing law, which actions are supported by the strength of valid evidence and he can be accounted for. Such thinking is in accordance with the application of the principle of legality in our criminal law, namely as explicitly formulated in Article 1 paragraph (1) of the Criminal Code "Nullum delictum nulla poena sine praevia lege poenali" or in other terms it can be known, "no criminal act, there is no crime, without the first rule of criminal law."

Cybercrime has various types, one of which is phishing. A phishing attack is a cybercrime in which users are tricked into sharing their personal data, such as credit card details, teller machines card details, passwords, and giving hackers access to their device, often without realizing it. Basically phishing is an infection that attacks a computer, cellphone or other device by tricking someone into downloading it. Next, the hacker traps the victim by using social engineering tactics to get the victim to click, share information, or download the file. Then the hacker will find out important information from the victim and use it to break into the victim's account, apply for an online loan or other crimes.

A phishing case occurred in Solo, Central Java, a private bank customer in Solo, Candraning Setyo, lost Rp72,653,000 in his savings account. The case has been reported to the Solo City Police. One of the victim's lawyers, Gading Satria Nainggolan, said the case his client experienced began in June 2020. At that time, Candra's husband's cellphone number suddenly lost signal. The mobile number is connected to the internet banking of the bank where Candra is saving. As long as the mobile number is inactive, a new subscriber identity module card has been issued to an unknown person. Then there is a suspicious transaction in the victim's account 5 strange transactions on June 11, 2020, at 13.24 west indonesian time to 13.32 west indonesian time. There are transfers to two bank accounts for Rp25,000,000 each, then there are three top ups (to digital financial service providers) of Rp9,801,000, Rp9,901,000, and Rp2,951,000.

II. Research Method

The research approach used in this research is qualitative research, while the type of The type of research used is empirical legal research. Empirical legal research is method that functions to see the law in a real sense and examines how the law works in the community (Asyraini et al., 2022; Octiva, 2018; Pandiangan et al., 2018).

The technique used is interview technique and document study. Interview is a question and answer activity orally to obtain information. The form of information obtained is stated in writing, or recorded audio, visual, or audio visual. Interviews are the main activity in observational studies (Octiva et al., 2018; Pandiangan, 2022; Pandiangan, 2018). Document study is a data collection technique that is not directly addressed to the research subject in order to obtain information related to the object of research (Octiva et al., 2021; Pandiangan et al., 2022).

Analysis of the data used is qualitative data analysis. Where the data analysis technique here focuses on non-numeric information, and discusses it conceptually without the numbers in it (Pandiangan et al., 2021). Qualitative data analysis involves the identification, examination, and interpretation of patterns and themes in textual data and determines how these patterns and themes help answer the research questions at hand (Pandia et al., 2018; Pandiangan, 2015; Tobing et al., 2018).

III. Results and Discussion

Electronic transactions can be classified as activities that cannot be separated from the human factor and the legal consequences of social communication in cyberspace. Today, electronic transactions can be found in all areas of society and making different lifestyles easier and more efficient. In addition, there has also been a change in the perspective on science where humans can communicate directly resulting in more widespread and the emergence of lawsuits and new cases related to electronic transactions. Activities included in legal actions or legal events related to technology and information commonly referred to as technology activities with electronic media or cyberspace, where legal actions and legal events are carried out almost without face-to-face or direct communication, but legally these activities can be classified as an act that is legally binding on the parties.

Electronic transaction activities have been regulated in the Preamble of the 1945 Constitution of the Republic of Indonesia that one of the goals of the state is "to prosper the life of the nation". This means that electronic transactions must be a profitable activity and certainly can be a way for the economic development of society with activities that take place between individuals and between individuals, between sellers and buyers or between individuals and institutions.

The existence of electronic transactions in addition to providing a positive impact for its users, is also a negative impact. There is no denying that electronic transactions will be an effective and efficient way for the public as users to commit crimes. People who have bad faith in the use of electronic transactions from the beginning make electronic transactions a place or medium for committing crimes. Crimes committed in the online world are called cybercrime.

One of these crimes that often occurs, especially in the banking sector, is Phishing. Phishing in the banking sector is considered a crime that uses social engineering techniques in an effort to deceive victims or customers in order to obtain personal data such as credit card details, mobile banking passwords and usernames (Radiansyah, 2016). Phishing perpetrators in the banking sector are often found to be insiders or employees of the banking institutions that are targeted. Various efforts have been made by the banking employee with his position as the main actor or as a person who helps in publishing customer or victim data (Yustitiana, 2021).

Law enforcement activities are all activities intended so that the law as a set of normative rules that regulates and binds legal subjects in all aspects of social and state life is truly obeyed and truly carried out as it should, in the narrow sense of law enforcement regarding enforcement activities against every violation. against laws and regulations, in particular narrowly through the criminal justice process that involves the role of law enforcement officers such as the police, prosecutors, advocates or lawyers and other judicial bodies. Law enforcement against perpetrators of criminal acts of theft of banking customer data is an effort made by law enforcement officials to eradicate criminal acts of theft of banking customer data by skimming methods that are detrimental to the state and society. Eradication of criminal acts of theft of banking customer data is closely related to law enforcement by law enforcement officers. Efforts to enforce criminal law in understanding the legal system include the operation of components of legislation or substance, law enforcement officers or legal structures and culture.

Law enforcement against perpetrators of criminal acts of theft of banking customer data requires the participation of the community in addition to the role of law enforcement officers, this shows that in law enforcement efforts the participation of all parties is needed

so that law enforcement runs effectively. The law that grows and develops in a certain area is the result of the process of community interaction, this law is intended to regulate people's lives in order to achieve peace and tranquility.

The results of the study indicate that Indonesia itself already has laws and regulations relating to electronic transactions ranging from the running of electronic transactions to the regulation of crimes, especially those related to banking such as phishing. These laws and regulations include:

3.1 Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions

The Law on Information and Electronic Transactions (hereinafter referred to as UU ITE) and the Government Regulation on the Implementation of Electronic Systems and Transactions explain that the definition of electronic transactions is "a term for legal acts carried out using computers, computer networks and/or other electronic media." The ITE Law contains material that adheres to two regulatory models. First, the regulation that is made narrowly selects the legal content material so that the things regulated in the specific content material are only certain. Second, the ITE Law has a comprehensive nature where the content it regulates includes things that follow developments and are in accordance with current needs. So in this case the ITE Law can cover various legal aspects, both material civil and civil and criminal procedural law, which will usually include evidence in criminal law.

In Indonesia, Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 becomes a complementary regulation in electronic transaction activities in Indonesia. Furthermore, the ITE Law regulates virtual-based crimes such as defamation, to crimes in banking electronic transactions, such as those currently being discussed, namely phishing.

The ITE Law has categorized that Phishing is a crime committed by manipulating, changing, eliminating and destroying electronic information and/or electronic data so that it can be considered as authentic data. This matter has been regulated in Article 35 of the ITE Law, in addition to other articles used to regulate the crime of phishing electronic transactions, namely Articles 32, 34, 35 and 36 which explain that what is done by phishing perpetrators is an act of fraud through various methods damage, change, or eliminate authentic data with the aim of harming other parties.

The ITE Law is considered to be an appropriate regulation in regulating the crime of phishing in electronic transactions, because the content of this law is a limitation that can be applied to the public regarding what can and cannot be done in virtual-based activities including transactions electronic.

3.2 The Book of Criminal Law

The Criminal Code is one of the other arrangements that can be used in the settlement of the crime of phishing electronic transactions. Although in the Criminal Code the crime of phishing does not specifically mention that the related act is an electronic transaction crime. Efforts have been made to deal with the crime of phishing, the Criminal Code criminalizes the crime of phishing through extensive interpretation methods or similarities to articles that are considered to still be included in the category of electronic transaction crimes, such as theft, embezzlement, insult to defamation whether it is done without the boundaries of the area and the place where the act takes place. The articles used in dealing with the crime of Phishing are Article 362 which explains the crime of

Phishing with the aim of stealing credit card numbers and Article 378 which explains the crime of Phishing through the website as a tool.

In this regard, the crime of phishing electronic transactions is usually not carried out by one person, but is carried out by two or more people who will assist in carrying out the phishing action. Therefore, usually, the Criminal Code will apply Article 363 paragraph (4) and Article 55 of the Criminal Code regarding participation in the settlement of the Phishing crime case. The presence of the Criminal Code in the settlement of cases of electronic transaction crimes is considered as one of the efforts to fill the legal vacuum. The application of the Criminal Code in the settlement of the crime of phishing electronic transactions is one of the ways of criminal policy through the means of criminal law, so that it is related to the crime of electronic transactions which indeed in its policies and regulations have a link between the ITE Law and the Criminal Code, then the arrangement will be included in a criminal law formulation policy or the so-called penal policy.

3.3 Government Regulation Number 71 of 2019 Concerning the Implementation of Electronic Systems and Transactions

Government Regulation Number 82 of 2012 concerning the Implementation of the Electronic Transaction System is a companion arrangement that goes hand in hand with the ITE Law. This government regulation contains legal provisions that specifically regulate the types of activities in the implementation of electronic transactions. As stated in the content of this regulation, it is explained that the implementation of electronic transactions in Indonesia is divided into two based on their nature, namely public and private. Electronic transactions of a public nature include the implementation of electronic transactions by agencies or other parties that provide public services as long as they are not excluded from the ITE Law, while private electronic transactions include electronic transactions carried out between business actors, between individuals, between agencies or between agencies and business actors.

However, this government regulation is considered irrelevant to the current conditions where virtual-based crimes such as electronic transactions are increasingly rampant. Therefore, the regulations related to the implementation of electronic transactions were amended by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and Government Regulation Number 80 of 2019 concerning Trading through Electronic Systems which also regulates personal data. This government regulation ultimately becomes more relevant because it is appropriate and meets the requirements in carrying out electronic transaction activities in accordance with the times and human factors as a reference.

3.4 Law Number 10 of 1998 Concerning Amendments to Law Number 7 of 1992 Concerning Banking

The Banking Act is one of the special laws and regulations used in the crime of phishing banking-based electronic transactions. The crime of data theft through online banking, mobile banking and credit card numbers are some of the crimes of phishing electronic transactions that often occur in banking institutions as the main target for phishers to get financial benefits.

The condition of Indonesia, which is currently being hit by the COVID-19 pandemic, has finally made banking transactions that were originally through face-to-face now replaced with an electronic or virtual-based transaction system. The categories of electronic banking services that are often targeted by the crime of phishing electronic

transactions and using the Banking Law in their settlement include electronic money, e-wallet, mobile banking, and mobile money transfers (Jazila, 2019).

The contents of the Banking Law explain the restrictions on the implementation of banks in carrying out their duties and authorities. The nature of the bank, which is a public fund depository, automatically has an obligation to maintain customer trust, especially with regard to personal data that will involve the use of customer funds. In this case, the Bank must be able to control or inhibit the existence of actions that are deemed to result in an unlawful act and damage the customer's trust in the bank.

Several electronic transaction arrangements contained in the Banking Law are related to the confidentiality of customer personal data, bank supervision in the operation of the electronic transaction system and business activities or programs from banks related to electronic transactions. Furthermore, in relation to the crime of phishing electronic transactions, the Banking Law will use Article 40 which explains the obligations of banks to protect customer personal data. In addition, there is Article 47 paragraph (1) which explains related to the sanctions that will be received if the bank or other party intentionally uses customer's personal data in committing a crime.

The sentencing process for the perpetrators is intended to provide a deterrent effect and ensure the entire security of internet banking application users contained in the terms and conditions section which contains the rights and obligations of customers and banks. However, in the explanation of these terms and conditions it is a standard agreement made in writing by the business actor/bank, so that the bank prioritizes the obligations of the customer and the rights of the bank rather than the rights of the customer and the obligations of the bank itself. It is hoped that in the future there will be no more mistakes, errors or omissions made by customers, from the bank and other threats.

In any device that uses Information Technology, the security system must be adequate so that it is not misused by the responsible party. Customer data as one of the banking equipment that uses information technology must also be accompanied by an appropriate security system against illegal acts by other parties. Theft of customer data is one of the data leaks caused by the weakness of the Bank's security system. As is well known, theft of customer data is regulated in the ITE Law. The provisions of Article 30 paragraph (3) of the ITE Law stipulates that "Everyone intentionally and without rights or against the law accesses Computers and/or Electronic Systems in any way by violating, breaking through, exceeding, or breaking into the security system."

Customer data on mobile banking accounts does not stop at only being limited to access to mobile banking accounts, but will also control accounts that contain a number of funds in the mobile banking account. Thus, it can be ascertained that the perpetrator will transfer the funds in the mobile banking account under his control. Such actions have also been regulated in the Funds Transfer Act. The provisions of Article 81 of the Invitation Number 3 of 2011 concerning Funds Transfer stipulates that "Everyone who unlawfully takes or transfers part or all of the Funds belonging to another person through a fake Funds Transfer Order shall be punished with imprisonment for a maximum of 5 (five) years or a fine a maximum of Rp5,000,000,000.00 (five billion rupiah)."

Criminal provisions that can be used to ensnare Cyber Crime perpetrators are only limited to the laws and regulations of the Criminal Code (KUHP) and Law Number 19 of 2016 concerning Information and Electronic Transactions. Other provisions, if any, are spread over various laws and regulations and are not specific. While America already has a number of laws and regulations that strictly regulate Cyber Crime, for example Title 18 U.S. Code 1030 which regulates Fraud and related activity in connection with computers, regulates Fraud Bank and Title 18 U.S. Code 2252B which regulates misleading domain

names on the internet. In addition, America is also a member of the Convention on Cyber Crime (Budapest Convention 2001) which is an organization that wishes to protect the public from crimes in the international world (Shahrullah, 2014).

IV. Conclusion

The results of the study indicate that Indonesia itself already has laws and regulations relating to electronic transactions ranging from the running of electronic transactions to the regulation of crimes, especially those related to banking such as phishing. The sentencing process for the perpetrators is intended to provide a deterrent effect and ensure the entire security of internet banking application users contained in the terms and conditions section which contains the rights and obligations of customers and banks.

References

Asyraini, Siti, Fristy, Poppy, Octiva, Cut Susan, Nasution, M. Hafiz Akbar, & Nursidin, M. (2022). Peningkatan Kesadaran Protokol Kesehatan di Masa Pandemi Bagi Warga di Desa Selamat Kecamatan Biru-biru. *Jurnal Pengabdian Kontribusi (Japsi), 2*(1), 33-36.

Jazila, Humada. (2019). *Jenis-jenis Sistem Transaksi Elektronik yang Berlaku di Indonesia*. Accessed on 22 April 2022 https://www.pikirantrader.com/finansial/10128-jenis-jenis-sistem-pembayaran-elektronik-yang-berlaku-di-indonesia.

Octiva, Cut Susan. (2018). *Pengaruh Pengadukan pada Campuran Limbah Cair Pabrik Kelapa Sawit dan Tandan Kosong Kelapa Sawit terhadap Produksi Biogas*. Tesis. Medan: Fakultas Teknik, Program Studi Teknik Kimia, Universitas Sumatera Utara. https://repositori.usu.ac.id/bitstream/handle/123456789/12180/157022002.pdf?sequence=1&isAllowed=y.

Octiva, C. S., Irvan, Sarah, M., Trisakti, B., & Daimon, H. (2018). Production of Biogas from Co-digestion of Empty Fruit Bunches (EFB) with Palm Oil Mill Effluent (POME): Effect of Mixing Ratio. *Rasayan J. Chem., 11*(2), 791-797.

Octiva, Cut Susan, Indriyani, & Santoso, Ari Beni. (2021). Effect of Stirring Co-digestion of Palm Oil and Fruith for Biogas Production to Increase Economy Benefit. Budapest *International Research and Critics Institute-Journal, 4*(4), 14152-14160. DOI: https://doi.org/10.33258/birci.v4i4.3521

Pandia, S., Tanata, S., Rachel, M., Octiva, C., & Sialagan, N. (2018). Effect of Fermentation Time of Mixture of Solid and Liquid Wastes from Tapioca Industry to Percentage Reduction of TSS (Total Suspended Solids). *IOP Conference Series: Materials Science and Engineering, 309*, 012086. DOI: 10.1088/1757-899X/309/1/012086.

Pandiangan, Saut Maruli Tua. (2015). *Analisis Lama Mencari Kerja Bagi Tenaga Kerja Terdidik di Kota Medan*. Skripsi. Medan: Fakultas Ekonomi dan Bisnis, Program Studi Ekonomi Pembangunan, Universitas Sumatera Utara. https://www.academia.edu/52494724/Analisis_Lama_Mencari_Kerja_Bagi_Tenaga_Kerja_Terdidik_di_Kota_Medan.

Pandiangan, Saut Maruli Tua. (2018). *Analisis Faktor-faktor yang Mempengaruhi Penawaran Tenaga Kerja Lanjut Usia di Kota Medan*. Tesis. Medan: Fakultas Ekonomi dan Bisnis, Program Studi Ilmu Ekonomi, Universitas Sumatera Utara.

http://repositori.usu.ac.id/bitstream/handle/123456789/10033/167018013.pdf?sequence=1&isAllowed=y.

Pandiangan, Saut Maruli Tua, Rujiman, Rahmanta, Tanjung, Indra I., Darus, Muhammad Dhio, & Ismawan, Agus. (2018). An Analysis on the Factors which Influence Offering the Elderly as Workers in Medan. *IOSR Journal of Humanities and Social Science (IOSR-JHSS), 23*(10), 76-79. DOI: 10.9790/0837-2310087679. http://www.iosrjournals.org/iosr-jhss/papers/Vol.%2023%20Issue10/Version-8/K2310087679.pdf.

Pandiangan, Saut Maruli Tua, Resmawa, Ira Ningrum, Simanjuntak, Owen De Pinto, Sitompul, Pretty Naomi, & Jefri, Riny. (2021). Effect of E-Satisfaction on Repurchase Intention in Shopee User Students. *Budapest International Research and Critics Institute-Journal, 4*(4), 7785-7791. DOI: https://doi.org/10.33258/birci.v4i4.2697.

Pandiangan, Saut Maruli Tua, Oktafiani, Fida, Panjaitan, Santi Rohdearni, Shifa, Mutiara, & Jefri, Riny. (2022). Analysis of Public Ownership and Management Ownership on the Implementation of the Triple Bottom Line in the Plantation Sector Listed on the Indonesia Stock Exchange. *Budapest International Research and Critics Institute-Journal, 5*(1), 3489-3497. DOI: https://doi.org/10.33258/birci.v5i1.4016.

Pandiangan, Saut Maruli Tua. (2022). Effect of Packaging Design on Repurchase Intention to the Politeknik IT&B Medan Using E-Commerce Applications. *Journal of Production, Operations Management and Economics (JPOME), 2*(1), 15–21. http://journal.hmjournals.com/index.php/JPOME/article/view/442.

Radiansyah, Ikhsan. (2016). Analisis Ancaman Phising dalam Layanan Online Banking. *Jurnal Ekonomika Bisnis, 7*(1), 2.

Shahrullah, R, S. (2014). Tinjauan Yuridis Penanganan Kejahatan Siber (Cybercrime) di Sektor Perbankan Indonesia dan Amerika. *Journal of Judicial Review, 16*(2).

Tobing, Murniati, Afifuddin, Sya'ad, Rahmanta, Huber, Sandra Rouli, Pandiangan, Saut Maruli Tua, & Muda, Iskandar. (2018). An Analysis on the Factors Which Influence the Earnings of Micro and Small Business: Case at Blacksmith Metal Industry. *Academic Journal of Economic Studies, 5(*1), 17-23. https://www.ceeol.com/search/article-detail?id=754945.

Yustitiana, Rhesita. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phising Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan dengan Teori Efektivitas Hukum. *Jurnal Hukum Visio Justisia, 1*(1), 105.