International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 04 Issue 09 September 2021

DOI: 10.47191/ijsshr/v4-i9-01, Impact factor-5.586

Page No: 2272-2279

Regulation on Electronic System Security for E-Wallet in Order to Protect Consumers from Financial Loss Due to Cyber Fraud Based on Indonesian Law

Rahel Octora[1], P.Lindawaty S.Sewu[2], Jason Arnold Sugiono[3]

[1,2,3]Law Faculty, Universitas Kristen Maranatha, Jln.Suria Sumantri 65-Bandung, Indonesia.

ABSTRACT: Developments of technology brings out various types of digital financial innovations. Nowadays, we live in a cashless society, where transactions using cash money are minimized. Payments are currently made with electronic money, whether classified as e-money or e-wallet. This research focuses on the security issue of the e-wallet system, considering that there are still various cases of fraud in Indonesia, that result in the loss of the user's e-wallet balance. This research is a normative juridical research that uses secondary data in the form of primary legal materials, such as various relevant laws and regulations, and secondary legal materials (books and legal literature). The approach used are statutory approach and conceptual approach. Indonesian law has regulated the obligations of e-wallet providers to ensure the security system of user accounts. In the event of a cyber fraud case that results in a loss of balance, the provider plays a role in responding to consumer complaints, and providing explanations regarding the cause of the loss of balance. Cyber fraud perpetrators are criminally responsible based on violations of the Electronic Information Transaction Law.

KEYWORDS: E-Wallet, Security, Electronic System, Consumer, Cyber Fraud.

I. INTRODUCTION

Technological developments affect people's lives, including the implementation of payment transactions that utilize information technology. Previously, payment transactions depended on the existence of money. According to traditional economics knowledge, money is defined as a generally accepted medium of exchange. Money is a commodity that is accepted by general consent as a medium of economic exchange in which prices and values are expressed. [1] In the common parlance, money simply is a means of payment for which everyone can receive goods in an economy. [2]

In today's modern era, money is not only interpreted as a medium of exchange in the form of cash, but can be in the form of debit cards or credit cards, and the next development is the use of electronic money and electronic wallets. The development of digital financial innovation is often termed 'Fintech' or Financial Technology. The development of e-money and e-wallet is increasing along with the development of start-up businesses, and various marketplaces that facilitate e-commerce activities. Fintech digital wallets allow users to save money in the application and can be used for payment transactions at offline and online merchants.

Electronic wallet (e-wallet) is defined as a software application that allows users to store payment instrument data, make digital payment and to be used for various type of digital transaction. [3] E-wallet is useful for maximizing cashless payment. The working system of the e-wallet is start from the user downloading the application, fills the balance in the e-wallet account. The funds stored in the e-wallet can be used for transactions, and the balance will be reduced by the amount of the transaction value. The use of e-wallet has spread widely to various parts of the world, including Indonesia. There have been many companies engaged in this Fintech field. The presence of instant payments can reduce the need for credit cards and debit cards.

Electronic money has both positive and negative impacts. The positive impact is that it can increase company investment and real national output. In addition, it can also save someone's time to make transactions. Public consumption will also increase due to offers or discounts that are always offered in the e-wallet application. For the negative impact of using e-wallet, namely the demand for money in the community will decrease, and will reduce interest rates on the money market. [4]

[1] Katharina John, *Money, The Root of Global Trade,* Norderstedt, Germany, 2007, page 2.

[2] Katharina John, *Money, The Root of Global Trade,* Norderstedt, Germany, 2007, page 3.

[3] G.Sameer, N. Marie-Claude,and R.Kausik, Gauging the Disruptive Potential of Digital Wallets, Mc.Kinsey on Payments, Vol.8 No.21, 2015, page 3-11.

[4] Tri Apriyani, *E-wallet Alat Transaksi dan Pembayaran Zaman Now*, https://www.suara.com/yoursay/2019/12/19/140313/e-wallet-alat-transaksi-dan-pembayaran-zaman-now , accessed on 19 March 2020, 15.53 Western Indonesian Time

Regulation on Electronic System Security for E-Wallet in Order to Protect Consumers from Financial Loss Due to Cyber Fraud Based on Indonesian Law

The issue to be investigated in connection with the widespread use of e-wallet in Indonesia is the potential fraud that results in loss of balance stored in a user's e-wallet account. In Indonesia, there is no clear regulation regarding parties who are obliged to guarantee the security of balances. As of the time of writing this article, the Deposit Insurance Agency has not been given the task by law to carry out guarantees for deposit funds in the form of e-wallet balances. [5]

Various cases of fraud that occur today are often associated with the issue of the e-wallet security system that must be guaranteed by the provider. On the other hand, the provider stated that security system is guaranteed. The loss of fund suffered by the account owner, occurred due to the user's own negligence to keep the One Time Password (OTP). The criminal offender targets the psychological aspect of the victim, by providing information that appears to be true, when in fact it is misleading information. When fraud has occurred, the criminal offender is usually difficult to trace.

Some examples of cases that occurred:

1. E-wallet balance belonging to Indonesian artist, Maia Estianty, lost due to fraud by someone claiming to be a motorbike driver in an online transportation corporation. The modus operandi of fraud is to state that his motorbike broke down, so he could not proceed with the food orders ordered by the victim. The perpetrator asked the victim to type the call forwarding code. The victim, who did not know it, then followed the direction of the perpetrator, resulting in the SMS data that entered the victim's cellphone in the form of OTP, also entered the perpetrator's cellphone. Armed with the OTP number, the perpetrator drains the victim's e-wallet balance.[6]

2. A syndicate of e-wallet burglars in South Sumatra. The Criminal Investigation Unit of the National Police on Monday (5/10/2020) arrested a syndicate. They breaking into bank customer accounts and e-wallet which integrated with the online transportation application (Grab). In this case, the perpetrators can steal money by asking the victim's One Time Password (OTP). They stole about 21 billion rupiah from thousands of victims. [7]

To overcome this problem, we have to analyze whether existing regulation in Indonesia has guaranteed the consumer protection, related to e-wallet security issue. The law should also regulate risk management system and fraud mitigation system both in the scope of detection and prevention of fraud.

The problems identified in this paper are:

1. How do the laws and regulations in Indonesia regulate the obligations of e-wallet providers in ensuring the security of electronic systems?
2. What is the role of the e-wallet provider in solving cyber fraud cases that result in the loss of the user's balance?
3. How is criminal law enforcement carried out against cyber fraud perpetrators who have caused material losses to e-wallet users?

II. RESEARCH METHOD

This research is done by using normative juridical research method. This research is to find out how the positive law regulates a particular thing, event, or problem. [8] This is an analytical descriptive research that describes the fact or phenomenon, and then analyzes it. The data that used in this research is secondary data, classified as primary, secondary, and tertiary legal materials.[9] The data used in this study is secondary data, that obtained from other parties indirectly to support research. Primary legal materials in the form of legislation in (field of financial transactions and criminal legislation). The secondary legal materials used, consist of books (textbooks) written by influential legal experts, legal journals, opinions of scholars, legal cases, Tertiary legal materials include dictionaries and encyclopedias. The data collection technique done by conducting a literature study. All data are analyzed by using deductive logical pattern. The approach used is a statutory approach and a conceptual approach.

III. DISCUSSION

1. Indonesian Laws and Regulations Relating to E-Wallet Provider's Obligation to Guarantee Electronic System Security

In this section will be discussed how the laws and regulations in Indonesia regulate the obligation of the e-wallets provider to maintain the security system. Some of the related regulations include:

a. Bank Indonesia Regulation Number 18/40/PBI/2016 concerning Payment Transaction Processing.

[5] https://www.cnnindonesia.com/ekonomi/20201022080435-78-561333/lps-tak-jamin-saldo-uang-elektronik , accessed on 4 January 2021, 15.00 Western Indonesian Time.

[6] https://m.cnnindonesia.com/teknologi/20191227194052-192-460547/akun-gopay-maia-estianty-diretas-gojek-bantu-lapor-polisi, accessed on 4 January 2021, 15.00 Western Indonesian Time.

[7] https://m.antaranews.com/berita/1766309/sahroni-apresiasi-polri-ungkap-pembobol-akun-transportasi-daring , accessed on 5 August 2021, 16.00 Western Indonesian Time.

[8] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta : UI Press, 1986, page 45.

[9] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta : UI Press, 1986, page 10.

Specific regulation related to transactions with electronic wallet is Bank Indonesia Regulation Number 18/40/PBI/2016 concerning Payment Transaction Processing. In the regulation, in order to be able to carry out transaction activities, payment system service providers, including electronic wallet operators must have a permit.

In Article 4 paragraph (1) it is stated that Every party acting as payment system service provider as referred to in Article 3 paragraph (1) must first obtain permission from Bank Indonesia.

To obtain permission, the Electronic Wallet Operator must first meet various requirements related to the feasibility aspect of the requirements (Article 9). Such requirements are: aspects of system safety and reliability, aspects of consumer protection.

b. Financial Services Authority Regulation Number 13/POJK.02 of 2018 concerning Digital Financial Innovation in The Financial Services Sector

This regulation regulates the activity in the digital financial transaction ecosystem. Digital financial providers that issue digital financial services/products must be subject to these rules. In relation to system security, based on Article 18 letter d, the organizer must conduct self-monitoring in connection with the confidentiality of consumer data and information.

Similarly, based on Article 22 paragraph (4), the Financial Services Authority conducts monitoring of the relevant operators with: aspects of security and confidentiality of consumer data and transactions, as well as aspects of standards and security of the platform.

c. Bank Indonesia Regulation Number 20/6 of 2018 concerning Electronic Money.

Article 18 of this Regulation states that one of the aspects that must be fulfilled by the Electronic Money Providers in order to obtain an operating license is related to the requirements of system safety and reliability. Article 34 states that in carrying out its activities, electronic money providers must pay attention to information system security standards.

Article 36 is set forth in detail on how the implementation of information system security standards, including the obligation to conduct information system audits by independent security auditors periodically at least once every 3 (three) years or every significant change. Article 37 paragraph (2) regulates the improvement of electronic money transaction security standards as applied through the use of authentication of at least 2 (two) factors (two factor authentication)

From these conditions, related to the rise of fraud cases in electronic wallets that causing consumer financial losses, this paper will try to analyze the regulation related to the security and reliability requirements of the system, as well as regulation related to consumer protection.

Electronic wallet providers basically carry out their functions based on the trust of the consumers. In the event that the electronic wallet providers fail to ensure the security of the system, especially in relation to the protection of funds belonging to the user, it may cause the user will not continue to use the electronic wallet service. This may threaten the business continuity of the electronic wallet service provider. As such, system reliability and security are crucial.

The reliability and security of the system is explained in Article 20 of Bank Indonesia Regulation Number 18/40/PBI/2016 PBI where the Electronic Wallet Provider needs to meet various standards in order to ensure the security of its information system. The Obligations of the Electronic Wallet Provider are:

a) fulfillment of general and system safety and reliability certifications and/or standards established by Bank Indonesia or related authorities/institutions; with regard to: security of user data and information as well as data and information of payment instruments stored in electronic wallets; system and procedures for activation and use of electronic wallets; and application of fraud detection system.
b) maintenance and improvement of technology security; and
c) the implementation of audits held periodically at least once every 3 (three) years or every significant change.

It also deals with consumer protection. In Law No. 8 of 1999 Article 4a, stated that consumers have the right to comfort, security, and safety in consuming goods and/or services. In the context of using e-wallets, consumers have the right to be guaranteed security for the balance / money stored in the e-wallet account.

To ensure the standard of system security, in Bank Indonesia Circular Letter Number 18/ 41 /DKSP dated December 30, 2016 concerning the Processing of Payment Transactions, electronic wallets must be audited.

The audit report should illustrate that the provider applies technology security systems, which are carried out effectively and efficiently with regard to compliance with laws and regulations. The security system, at least meet the principles of:

1. confidentiality
2. integrity

3. two factor authentication
4. non-repudiation
5. availability

Bank Indonesia supervises Electronic Wallet Providers. The supervision is indirect supervision, in which the Electronic Wallet Providers is required to submit reports both routine and incidental. This is regulated in Bank Indonesia Circular Letter Number 18/41 /DKSP dated December 30, 2016 Regarding the Implementation of Payment Transaction Processing.
In section VIII concerning Supervision and Reports on the Implementation of Payment System Service Activities, it is stated that Electronic Wallet Providers are required to submit information regarding the occurrence of fraud.
Quarterly reports that at least contain information regarding the recording and handling of fraud that occur in the form of: a) frequency of occurrence; b) causes of fraud; and c) the value of losses due to fraud.
In addition, the occurrence of fraud can also be submitted in an incidental report. The report contains information related to chronology and the impact of losses caused.
Based on the description above, it appears that Bank Indonesia and the Financial Services Authority have imposed strict provisions regarding the obligations of electronic wallet providers to ensure the reliability of their electronic systems in order to ensure that the amount of money belonging to consumers is stored safely.
Until now, the fraud that has occurred has occurred because users are easily manipulated by irresponsible people. The two-factor authentication mechanism is basically a mechanism to ensure that the party who enters the system is the one who really has the right.
Based on research conducted by a research team from Brigham Young University, Two-factor authentication can be explained as follows:
Two-factor authentication requires users to present two of the following types of authentication factors:
1. Something they know (traditionally a password)
2. Something they have (such as a phone or hardware token)
3. Something they are (referring to biometrics, such as a fingerprint)
Two-factor authentication provides a strong defense against account compromise. The number of recent password database leaks underscores the risk of account compromise. Because users tend to reuse the same username and password across multiple sites password leaks from a single site can lead to a chain-reaction of account compromises as attacker access other accounts with the same credentials. [10]

With the implementation of a security system that is in accordance with standards, in this case it is necessary to further investigate how fraud can occur. Below are some examples of cases in Indonesia, summarized from consumer complaints:

1. A case of breaking into an OVO balance, where the perpetrator accesses the victim's e-mail, then the perpetrator changes the victim's e-mail and cellphone number registered for the OVO account, so that the victim can no longer access his account. The perpetrator then took the victim's balance. This case occurs even though the security system implemented by OVO is sms verification, passcode, and fingerprint.[11]
2. The user's GoPay balance is deducted for transactions made by other people (actors). The perpetrator made a purchase of a paid application through the Playstore using the perpetrator's e-mail, and paid for the transaction using the victim's GoPay account.[12]

The cases above are suspected to have occurred because the perpetrators were able to illegally access the victim's e-mail account so that the perpetrator could take over the electronic wallet account and use the victim's money against the law.
Thus, the laws and regulations in Indonesia have actually provided adequate regulations related to system security on electronic wallets. This cyber fraud case can occur because of the cleverness of the perpetrator in manipulating the victim, as well as the carelessness of the victim that cause financial losses.

2. The Role of the E-Wallet Provider in the Settlement of Cyber Fraud Cases based on the Laws and Regulations in Indonesia
In this section, will be explained how the E-Wallet provider must act in the context of solving cyber fraud cases that harm consumers.

[10] Ken Reese, *et.al*., A Usability Study of Five Two-Factor Authentication Methods, Proceedings of the Fifteenth Symposium on Usable Privacy and Security, p.357.
[11] https://mediakonsumen.com/2019/06/27/surat-pembaca/ovo-tidaklah-aman-saldo-ovo-saya-kebobolan , accessed on 5 August 2021, 17.00 Western Indonesian Time.
[12] https://mediakonsumen.com/2021/01/06/surat-pembaca/saldo-gopay-saya-hilang-tidak-jelas-gojek-tidak-bertanggung-jawab , accessed on 5 August 2021, 19.00 Western Indonesian Time.

Consumers who experience cases of cyber fraud that cause them losing a certain amount of money stored in their e-wallet accounts, will usually contact the e-wallet provider to question the case and seek a resolution.

Based on the Consumer Protection Law, in the event of a case that harms consumers, business actors must provide a complaint mechanism. As regulated in Article 4 letters d and e of the Consumer Protection Law, consumers have the right to have their opinions and complaints heard on the goods and/or services used, and the right to get advocacy, protection, and efforts to resolve consumer protection disputes properly.

From a consumer interest point of view, consumers want lost funds to be recovered. However, the e-wallet provider will not simply return the lost funds. This causes disappointment in consumers where consumers feel aggrieved by the e-wallet. In this case, to answer how the e-wallet provider should play a role in solving cyber fraud cases that harm consumers (based on applicable laws in Indonesia), the analysis will start from the legal relationship that occurs between the consumer and the e-wallet provider.

E-Wallet Providers are business actors engaged in digital payment services. E-Wallet consumers are service users who are also entitled to legal protection and are entitled to various fulfillment of consumer rights as guaranteed by law.

The legal relationship that occurs between the provider and the consumer is based on an agreement. The agreement is an electronic contract that contains terms and conditions that must be agreed by consumers before using the digital wallet application. The contents of these terms and conditions are determined unilaterally by the provider. The contract is a standard contract that contains standard clauses. In the contract, the provider also applies an exoneration clause which limits the liability of the provider in the event of potential loss to the consumer.

Article 1 number 10 of Law no. 8 of 1999 concerning Consumer Protection defines standard clauses as any rules or conditions and conditions that have been prepared and determined in advance unilaterally by business actors as outlined in a document and/or agreement that is binding and must be fulfilled by consumers.

Based on these provisions, the standard agreement contains standard clauses that have been determined unilaterally by business actors and are no longer negotiable by consumers. The clauses contained in an agreement refer to matters of a business or economic (financial) nature that incriminate one of the parties. This makes it vulnerable to inequality between consumers and business actors.[13]

An exoneration clause is a clause in an agreement, which stipulates an exemption or limitation from certain responsibilities, which normally according to law should be his responsibility. [14]

In the case of cyber fraud against e-wallet users, we need to analyze first, what responsibilities normally according to law are the responsibility of the provider. To answer this, the concept of obligation and responsibility will be presented in the context of consumer protection law.

The obligations of business actors are contained in Article 7 of the Consumer Protection Law which regulates the following:

The obligations of business agents shall be:

a) having a good intention in conducting business activities;
b) providing correct, clear and honest information about the condition and guarantee of goodsand/or services and providing explanation about uses, repair and maintenance;
c) treating or serving consumers correctly and honestly and indiscriminative
d) guaranteeing the quality of the goods and/or services produced and/or traded on the basis of the prevailing standard provisions on the quality of goods and/or services;
e) providing an opportunity to consumers to test and/or try certain goods and/or services and providing an assurance and/or a guarantee for the goods made and/or traded;
f) giving compensation and or refund for the losses caused by the use, application and utilization of goods and/or services traded;
g) giving compensation and/or refund if the goods and/or services received or utilized are not up to the agreement

While the matter of liability, is a different concept from the concept of obligation. Liability refers to the consequences that must be borne when there is a loss to another party, for example, to pay compensation for losses incurred by other parties, due to the actions we have done and on the part of the perpetrators, there is an element of fault.

For the context of using e-wallet, several important points that can be raised are:

1. The e-wallet provider must carry out its obligations. In the event of a breach of obligations, this may result in legal consequences. In the case of loss of funds in the e-wallet account, the obligations of the provider as a business actor are:

[13] Agus Satory, *Perjanjian Baku Dan Perlindungan Konsumen Dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan Dan Implementasinya Di Indonesia.* Padjadjaran Jurnal Ilmu Hukum (Journal Of Law) 2(2), 2015, page 269–90.

[14] Zakiyah, *Klausula Eksonerasi Dalam Perspektif Perlindungan Konsumen.* Jurnal Universitas Lambung Mangkurat , ISSN 1979-4940, 2017, page. 437.

a) Providing complaint services (accommodating and recording complaints submitted by consumers and submitting them to the relevant divisions)
b) Provide information/explanation on cases of loss of balance experienced by consumers, related to the causes, on the validity of the transaction, and on the fault of which party may cause the loss to occur, based on data recorded in the e-wallet provider's electronic system.
c) serve consumer complaints by not discriminating. In practice, it is still found when consumers who submit complaints are public figures, business actors respond quickly, while when consumers come from ordinary people, cases are left without any clarity.
d) provide compensation if it is proven that the loss of balance is the result of a system error on the part of the provider.
e) If it turns out that the fault is not with the e-wallet provider, the provider should provide recommendations/advice to consumers regarding which party the consumer should take legal action against.

2. In fact, the e-wallet provider does not feel obliged to carry out these things, because the provider has set the exoneration clause as follows:

a) that the provider states that it is not responsible for consumer losses, if such losses occur due to consumer fault.
b) That the provider has the right to correct the balance if according to the provider's observations there are suspicious transactions.
c) that the provider will only be responsible if it is proven that the fault lies with the provider.
d) That the consumer has understood the risk of loss of balance, account takeover and fraud. Therefore, consumers are obliged to maintain the confidentiality of the security code and OTP.
e) That the consumer frees the provider from all claims if the consumer fails to maintain the confidentiality of the OTP.

3. To demand the responsibility of the provider, the consumer must be able to prove the fulfillment of fault on the part of the provider. In this case, the consumer bears the burden of proof, so that the consumer must be able to provide information not only about the losses suffered, but also regarding system errors or system insecurity. This will certainly make it difficult for the consumer in the consumer dispute resolution process.

Based on the description above, it can be concluded that based on the Consumer Protection Law in force in Indonesia, the e-wallet provider has a role in facilitating the resolution of the problem of losing balances experienced by consumers. The e-wallet provider is not legally responsible if it can be proven that the loss of balance did not occur due to the provider's fault. The thing that needs to be considered in responding to consumer complaints is the principle of non-discrimination, in which providers may not apply different treatment to consumers based on the social status of consumers or the reputation of consumers in the community.

3. Criminal Law Enforcement Problems on Cyber Fraud against E-Wallet

Cyber fraud is an example of cyber crime. David S.Wall mentioned "cybercrime broadly describes the crimes that take place within that space and the term has come to symbolize insecurity and risk online." [15] Cybercrime, like crime, consist of engaging in conduct that has been outlawed by a society because it threatens social order. As we will see, most of cybercrime we see today simply represents the migration of real world crime into cyberspace. [16] Graham defines e-fraud as "a fraudulent behavior connected with computerization by which someone intends to gain dishonest advantage". In this definition e-fraud equates to, and supersedes, the term computer fraud.[17]

Cases of loss of balance in e-wallet user accounts can occur as a result of cyber fraud committed by criminals. The legal relationship between the e-wallet provider and the user/consumer is a private legal relationship, as explained in the previous section. In the event of an illegal withdrawal of funds by a third party, in this case the perpetrator of the burglary can be considered to have committed a crime so that criminal law enforcement is needed.

Criminal law is a part of public law. Criminal Law can be defined as rules that regulate action of legal subject, which establish the rights and obligations, what individuals may or may not do, and also punishment for the violation.

In the Indonesian legal system, the determination of an act as a criminal act is based on the principle of legality, where the perpetrator of an act can be sanctioned on the basis of the prevailing written regulations. The principle of legality is clearly stated in Article 1 (1) of the Criminal Code that is currently prevail.

The perpetrators, commits the criminal act in such a way that consumers provide OTP to the perpetrator, and they can easily access the victim's e-wallet account. Thus, the e-wallet provider considers that the transaction is a legitimate transaction because the cyber fraud perpetrator has an authentication code or is authorized to make the transaction. Such actions are usually preceded by phishing.

[15] David S.Wall, *Cybercrime, The Transformation of Crime in the Information Age, Polity Press, United Kingdom, 2007* . page 10.
[16] Susan W. Brenner, *Cybercrime and The Law, Challenges, Issues and Outcomes,* Boston, Northeastern University Press, 2012, page 6.
[17] K. A. Akintoye, O. I. Araoye, *Combating E-Fraud on Electronic Payment System,* International Journal of Computer Applications (0975 – 8887) Volume 25– No.8, July 2011, page 50.

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords, and credit card details, by posing them as a trustworthy site in electronic communication. Phishing is typically carried out by an e-mail or by instant messaging, and often directs users to enter the details of website, although phone contact has also been used at many of the times. [18]

Based on the Indonesian legal system, the perpetrator's actions in illegally accessing the victim's account can be qualified as a violation of Article 30 paragraphs (1) and (2) which states:

(1) Every Person intentionally and without rights or against the law, accesses Computers and/or Electronic Systems belonging to other Persons in any way.

(2) Any person intentionally and without rights or against the law, accesses a Computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents

Article 47: Everyone who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp.800,000,000.00 (eight hundred million rupiah).

Criminal law enforcement focuses on the imposition of criminal sanctions on perpetrators as a form of liability. There's different focus from private law.

The state plays an active role in enforcing criminal law for cases of theft of e-wallet balances. In this case, the law enforcement process will follow the criminal procedural law that apply in Indonesia. One of the stages that must be passed is the stage of investigation. Based on Articles 102 and 106 of the Criminal Procedure Code, law enforcers can start the investigation process if law enforcers know or find a criminal act, or based on a report, or by accusation. Thus, the existence of a report becomes an important thing to start the law enforcement process.

In Indonesia, the police once arrested an e-wallet burglary syndicate that carried out its action by tricking the victim so that the victim gave the perpetrator an OTP code. The victim is an online motorcycle taxi driver. The case was then detected by the internal security system of the e-wallet provider and then the provider reported the crime to the Criminal Investigation Agency of the Indonesian National Police. Then the police managed to arrest the perpetrators and the perpetrators were processed according to the applicable legal provisions.

In reality, consumers who lose their e-wallet balance will consider various things before reporting the case to the police. The victim will initially seek a refund through the provider, but the provider will only make the return if it is proven that a system error has occurred. If the balance loss occurs due to the negligence of the consumer / victim in maintaining the confidentiality of the OTP, then in this case, the fault lies with the victim, so the funds will not be returned.

Victims hope that their funds can be returned, while reporting to the police is completely unrelated to the refund process, so many consumers choose not to process this case into criminal law procedure. This is one of the obstacles in law enforcement on cases of theft of e-wallet balances, because the lack of legal awareness of victims to report. It will result in more perpetrators not being arrested.

IV. CONCLUSIONS

1. Regulations in Indonesia have established obligations for e-wallet providers to ensure the security of their electronic systems, one of which is by using One Time Password. This is stated in the Bank Indonesia Regulation and Financial Service Authority Regulation. Providers who violate these obligations cannot continue their business activities, because the security of electronic systems becomes a requirement of issuing business licenses.

2. E-wallet providers are business actors who must provide customer complaint service, and provide explanations to consumers about the occurrence of cyber fraud cases that result in loss of consumer balance. There is no obligation for businesses to return lost money, as long as it can be proven that it happened not because of the provider's fault.

3. Law enforcement needs to be supported by public legal awareness. Law enforcement for cyber fraud against e-wallet users in Indonesia can be done based on victim reports. The more victims are reluctant to report, the more cases of cyber fraud that go unnoticed by law enforcement.

REFERENCES

1) Katharina John, *Money, The Root of Global Trade,* Norderstedt, Germany, 2007, page 2.
2) Katharina John, *Money, The Root of Global Trade,* Norderstedt, Germany, 2007, page 3.
3) G.Sameer, N. Marie-Claude,and R.Kausik, Gauging the Disruptive Potential of Digital Wallets, Mc.Kinsey on Payments, Vol.8 No.21, 2015, page 3-11.

[18]Akash Amal Mishra, *An Overview On Cybercrime And Security-Volume 1*, Tamil Nadu, Xpress Publishing, 2020, page 40.

4) Tri Apriyani, *E-wallet Alat Transaksi dan Pembayaran Zaman Now*, https://www.suara.com/yoursay/2019/12/19/140313/e-wallet-alat-transaksi-dan-pembayaran-zaman-now , accessed on 19 March 2020, 15.53 Western Indonesian Time
5) https://www.cnnindonesia.com/ekonomi/20201022080435-78-561333/lps-tak-jamin-saldo-uang-elektronik , accessed on 4 January 2021, 15.00 Western Indonesian Time.
6) https://m.cnnindonesia.com/teknologi/20191227194052-192-460547/akun-gopay-maia-estianty-diretas-gojek-bantu-lapor-polisi, accessed on 4 January 2021, 15.00 Western Indonesian Time.
7) https://m.antaranews.com/berita/1766309/sahroni-apresiasi-polri-ungkap-pembobol-akun-transportasi-daring , accessed on 5 August 2021, 16.00 Western Indonesian Time.
8) Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta : UI Press, 1986, page 45.
9) Soerjono Soekanto, *Pengantar Penelitian Hukum*, Jakarta : UI Press, 1986, page 10.
10) Ken Reese, *et.al*., A Usability Study of Five Two-Factor Authentication Methods, Proceedings of the Fifteenth Symposium on Usable Privacy and Security, p.357.
11) https://mediakonsumen.com/2019/06/27/surat-pembaca/ovo-tidaklah-aman-saldo-ovo-saya-kebobolan , accessed on 5 August 2021, 17.00 Western Indonesian Time.
12) https://mediakonsumen.com/2021/01/06/surat-pembaca/saldo-gopay-saya-hilang-tidak-jelas-gojek-tidak-bertanggung-jawab , accessed on 5 August 2021, 19.00 Western Indonesian Time.
13) Agus Satory, *Perjanjian Baku Dan Perlindungan Konsumen Dalam Transaksi Bisnis Sektor Jasa Keuangan: Penerapan Dan Implementasinya Di Indonesia.* Padjadjaran Jurnal Ilmu Hukum (Journal Of Law) 2(2), 2015, page 269–90.
14) Zakiyah, *Klausula Eksonerasi Dalam Perspektif Perlindungan Konsumen.* Jurnal Universitas Lambung Mangkurat , ISSN 1979-4940, 2017, page. 437.
15) David S.Wall, *Cybercrime, The Transformation of Crime in the Information Age, Polity Press, United Kingdom, 2007* . page 10.
16) Susan W. Brenner, *Cybercrime and The Law, Challenges, Issues and Outcomes,* Boston, Northeastern University Press, 2012, page 6.
17) K. A. Akintoye, O. I. Araoye, *Combating E-Fraud on Electronic Payment System,* International Journal of Computer Applications (0975 – 8887) Volume 25– No.8, July 2011, page 50.
18) Akash Amal Mishra, *An Overview On Cybercrime And Security-Volume 1*, Tamil Nadu, Xpress Publishing, 2020, page 40.