

Investigating *Online Fraud with the BRI Mobile Mode* : Modus Operandi and the Gaps in Law Enforcement

Febriansyah ¹, Musriko ²

5222220026@univpancasila.ac.id ¹, 5222220016@univpancasila.ac.id ²

^{1,2} Magister Ilmu Hukum, Universitas Pancasila, Indonesia

Article Info

Received: 2023-01-29

Revised: 2023-04-10

Accepted: 2023-06-20

Keywords:

Cybercrime; BRI Mobile
online fraud; *lex specialis*
derogate legi generali;
law enforcement

Abstract

*Cyber universe was made uproar by the actions of fraudsters posing as bank employees. Fake advertisements are a 'cover' for fraudsters in their efforts to 'drain' victims' money. In 2023, the South Jakarta District Court sentenced 9 perpetrators. this article, we will examine in depth the modus operandi used by the perpetrators, related to legal regulations. a critical assessment will be carried out regarding law enforcement carried out by the Public Prosecutor and the Panel of Judges. The author uses a legal research with statutory and regulatory policies and case approach to answer the problem. The results of the research show that the perpetrators used various modes, where each of these is an independent criminal act. It was found that there were gaps in the legal enforcement of this case, especially by the prosecutor, which included a lack of understanding regarding the ITE Law and other related regulations, as well as inconsistencies in the application of the *concurus realis* doctrine and sustainable actions, and there were indications of lack of seriousness in handling it, where Article 36 of the ITE Law which is the severity of punishment, is not applied in the indictment*

I. Introduction

The 1945 Constitution of the Republic of Indonesia is the supreme law that contains rules and norms that must be obeyed by all Indonesian people. It has also been stated in the 1945 Constitution of the Republic of Indonesia, that Indonesia is a country of law. In further understanding, it is stated that the State of the Republic of Indonesia and all elements of its government must be guided by legal principles (*rechtsstaat*), which are based on the interests of the nation and not based on the interests of certain parties (*machstaat*)¹.

One of the legal instruments that is closely related to the state's function in maintaining public security and order is the criminal law. Criminal Law is one of the legal instruments that runs in a country. Criminal law regulates the principles and contains rules to determine an act that is prohibited followed by criminal sanctions as a threat to every person who commits an act that has been prohibited, and determines the procedure for carrying out the crime when there is a person who violates the act as formulated.²

The rapid development of technology has had a significant positive impact, especially in the era of globalization like today. One of the positive impacts is to make it easy and fast for the wider community to obtain and provide information. In fact, at the same time, the public can find out what events are happening in other places. Not only that, just through a smartphone in hand, we can present pizza, masseuse, taxi or goods from online stores in just a few minutes.

Apart from the positive impact as mentioned earlier, this rapid technological development also has a negative impact. One of them is the emergence of new crimes along with the improvement of information technology, namely *Cybercrime*. *Cybercrime* can be translated as illegal activities carried out using computers through an internet network.³

Cybercrime is very closely related to *cyberspace*. *Cyberspace*, also known as cyberspace, is a communication medium that is located in a computer that is carried out using the internet. Space is a social space that is not limited by distance and time.⁴ The abuse that occurs in a *cyberspace* is then referred to as *cybercrime*.⁵ There are various types of cybercrime, including *online fraud*

Online fraud is a type of crime that uses technology in all its actions. The principle of *online fraud* is the same as ordinary fraud which is generally regulated in Article 378 of the Criminal Code, where in every case of fraud there will definitely be victims who are harmed and other parties who gain illegal benefits. The difference between *online fraud* and ordinary fraud lies in the use of electronic systems (telecommunication equipment, the

¹C.S.T. Kansil, *Ilmu Negara Umum dan Indonesia*, (Jakarta : PT Pradnya Paramita, 2001), 2.

²Moeljatno, *Asas-Asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2015), 1

³Lilik Muladi, *Seraut Wajah Putusan Hakim: Studi Kasus Prita Mulyasari*, (Jakarta : Rineka Cipta, 2009), 40.

⁴Maskun, *Cyber Crime: An Introduction*, (Jakarta: Kencana, 2013), 46.

⁵*Ibid.*, 47

internet and computers).⁶

In general, the regulation of a criminal act of fraud is contained in Article 378 of the Criminal Code. The article does not specifically regulate fraud in cyberspace, but regulates fraud in general (in the main form) which explains that fraud is an act committed by a person with the aim of obtaining unlawful profits for himself or others, by using a false name, by deception or a series of lies, to encourage others to give something to the prison. To provide debts or write off debts, they are threatened with fraud with a criminal threat in the form of imprisonment for a maximum of 4 years.

Fraud related to information and electronic transactions is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Although there is no provision in the ITE Law that explicitly uses the word "fraud" as used in Article 378 of the Criminal Code, if you look at the ITE Law, you will find several provisions that have a close meaning to "fraud", such as in Article 28 paragraph (1) of the ITE Law which uses the phrase "news bihong". Similar to conventional fraud, in *cyberspace* fraud is carried out with a variety of *modus operandi*, including, *Phishing, Scam, Account take over, Social engineering, Share login info*, and so on.

Of the many cases of *online* fraud that have occurred, there is one case that has been decided by the South Jakarta District Court and is quite interesting to study, namely as the case contained in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel. in this case the victim felt deceived and suffered considerable material losses after previously receiving *WhatsApp* from one of the defendants whose content seemed to contain information from Bank BRI with the sentence; "HI BRI FRIENDS, WITH THE CHANGE IN TARIFFS. etc". On that basis, the Panel of Judges stated that the defendants had been guilty of committing the crime "... *intentionally and without rights or unlawfully in any way transferring or transferring electronic information and/or electronic documents to the electronic system of another person who is not entitled ...*".

Based on this, the author is interested in examining and researching *how* the *modus operandi* used by online fraud perpetrators in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel, as well as *how Law Enforcement* against online fraud perpetrators both by the Public Prosecutor, and by the Judge as reflected in the Decision.

2. Research Method

Philipus M. Hadjon said that legal science has a distinctive character, namely in terms of its normative, practical, and precrisive nature.⁷ Departing from this, in this article, in order to be able to answer the formulation of the problem above, the author uses a type of

⁶Noor Rahmad, "Studi Hukum tentang Kejahatan Penipuan Online", Journal of Sharia Economic Law 3 no 2, (April 2019): 105. <https://doi.org/10.26618/j-hes.v3i2.2419> 103-117

⁷Mukti Fajar ND and Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Penelitian Hukum Empiris*, (Yogyakarta: Pustaka Siswa, 2010), 34

normative legal research (normative juridical), namely legal research that puts law as a normative system. The norm system in question is about principles, norms, rules, from laws and regulations, and court decisions.⁸ The focus of this research will be on matters related to legal systematics, namely identifying the main meaning in the law, including legal subjects, legal acts, legal events in relation to the application of legal principles, legal doctrines and laws and regulations. The approaches used by the author include the statute approach, and the case approach, especially the Jakarta District Court Decision South Number 274/Pid.Sus/2023/PN Jkt.Sel.

3. Results and Discussion

MODUS OPERANDI USED IN *ONLINE FRAUD* CRIMES AND THEIR LEGAL REGULATIONS

Online *fraud* is one of the cybercrimes that has been widely discussed in various studies, especially related to digital security and digital literature. The use of the term *online fraud* also varies, such as cyber fraud or digital fraud. Meanwhile, in the ITE Law, it does not use the preposition/term "fraud". From the discussion of the ITE Bill text, both at work meetings and hearings held by the House of Representatives of the Republic of Indonesia, most of them discussed protection from fraud but the context is more to customers, prize draws, credit card fraud, and *multi-level marketing fraud*.⁹

In principle, *online fraud* refers to a type of fraud using internet media such as chat rooms, electronic messages, or websites in conducting fraudulent transactions with financial institutions such as banks or other institutions with certain relationships.

On February 23, 2023, the Director General of Informatics Applications (Dirjen Aptika) of the Ministry of Communication and Informatics, Samuel Abrijani Pangerapan said: "*Our society is the easiest to be deceived online and online fraud is very high in Indonesia, reports to us last year have exceeded 130 thousand*"¹⁰

The modus operandi in the field of crime is the use of methods or techniques that show the special characteristics of a crime when committing an evil act¹¹. In other words, the modus operandi is a way of how the perpetrator of the crime commits his speech.

Online fraud is a type of crime whose number and mode are increasing rapidly along with the digitalization process in Indonesia. Based on the results of research conducted in 2022,

⁸*Ibid*, 17

⁹Anton Hendrik Samudra, "Modus Operandi dan Problematika Penanggulangan Kejahatan Penipuan Online", Jurnal Mimbar Hukum 31 no. 1, (2019), 68. <https://doi.org/10.22146/jmh.34786>. 59-74

¹⁰ Wahyu Sudoyo, "Kominfo Catat, Korban Penipuan Online Capai 130 Ribu di 2022". <https://infopublik.id/kategori/nasional-sosial-budaya/715547/catatan-kominfo-korban-penipuan-online-reach-130-thousand-at-2022>. (diakses 2 Januari, 2023)

¹¹Dirjosisworo, *Ruang Lingkup Kriminologi*, (Jakarta, Rajawali, 1984), 54

it shows that the public is very vulnerable to digital fraud, namely 98.3% of respondents (1,671 people) have received one or more digital fraud messages. The most common types of scam messages they received were gift scams (91.2%), illegal loans (74.8%), malware/virus link sending (65.2%), scams under the guise of a family crisis (59.8%), and illegal investments (56%).¹² The most common means of communication used in fraud is the mobile network (SMS/phone) (64.1%), which is very simple, inexpensive and is a basic feature of mobile phones, so its range can be very wide. This is followed by social networks (12.3%), chat apps (9.1%), websites (8.9%), and email (3.8%).¹³

Compiled from the opinions of Dam, Cross, and Puram, there are at least 14 (fourteen) types of digital fraud modes as described below¹⁴ :

1. *Phishing*. In particular, *phishing* is the theft of important information by tricking victims into accessing a fake website/page to trap victims. Usually, these criminals target paid streaming services, banks, e-commerce, and MSMEs.
2. *Scam*. In particular, this mode of fraud is often aimed at making money by deceiving others. It usually happens through communication with chat applications, telephones, and so on.
3. *Account take over*. Fraud takes over someone else's account suddenly, and victims often feel the consequences instantly in an instant.
4. *Social engineering*. This mode is an action that is carried out by utilizing human interaction. Scammers will use psychological engineering or manipulation to trick their targets into making digital security mistakes. \
5. *Share login info*. This mode is carried out with the intention of obtaining sensitive information from the victim's account such as OTP codes, PINs, and *passwords*).
6. *Share card info*. A fraudulent act that involves stealing card data information, both card numbers and OTP codes, from the issuing bank. The most common way to do this is to contact the victim on behalf of a bank or other related institution.
7. *ID theft*, namely specifically fraud by stealing the victim's identity card. This identity will then be used to create an account on the platform with someone else's identity
8. *Typosquatting*, which is a scam that involves registering a site's domain name that is very similar to an existing site but the site name is slightly different from the original site name (as if there was a typo or typo). This domain name is then used to trick internet users into thinking they are browsing the page of the website they are going to visit.
9. *Pharming*. Fraud involves taking control of the victim's computer system through hacking, malware, or software that takes the victim to a fake page where they are invited to enter their data
10. *Skimming*. A form of fraud in which the victim's personal information on an electronic card (such as a credit card) is retrieved through a device that is secretly embedded in the card reader.

¹²Novi Kurnia, Rahayu, et al, *Digital Fraud di Indonesia: Modus, Media, dan Rekomendasi*, (Jogjakarta: Program Studi Magister Ilmu Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Gadjah Mada, 2022), 5

¹³ *Ibid*, 23

¹⁴ *Ibid*, 22

11. *Malware*. Virus-like intrusion software is installed on a computer to alter the functionality of a program or document.
12. *Lottery Scams*. This mode begins when the victim receives an email from a source claiming that they have won a prize from an organization, and in order to receive the prize, the victim must reply to the email with certain information
13. *Video Scams*, is a fraudulent process that asks the victim to watch a video infected with a virus. When victims try to watch the video, they will be asked to download a codec to watch.
14. *Scareware*. An intruder program designed to trick users into buying and downloading various malicious software, such as fake anti-virus software.

In principle, *online* fraud refers to a type of fraud using internet media such as chat rooms, electronic messages, or websites in conducting fraudulent transactions with financial institutions such as banks or other institutions with certain relationships.¹⁵ As with fraud in general, in *online* fraud there are also a series of attempts at deception or with a series of lies from the perpetrator with the aim of "moving others" as the victim to hand over something of value to him.

In relation to *cyberspace*, these valuable things can be in the form of electronic information, electronic documents, or even access codes. An access code is the key to being able to access a computer and/or Electronic System which can be in the form of numbers, letters, symbols, other characters or a combination of these.¹⁶ Electronic System is a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate Electronic Information. Based on this, it can be seen that in an electronic system there is a lot of data and valuable information that can be targeted by perpetrators of fraud. In fact, in today's digital era, the use of paper money as a means of transaction has begun to shift to the use of electronic money, namely the value of money stored electronically in a medium such as a server. The value of electronic money is the value of money that is stored electronically on a medium that can be moved for the purpose of payment transactions and/or fund transfers.¹⁷ Therefore, when viewed from the storage media, electronic money is recorded on electronic media managed by banks or non-bank financial institutions. In this case, the owner of the money is given access by the bank to the use of the Electronic Money Value.¹⁸

Access codes are so important in electronic transactions, so it is not surprising that the perpetrators of crimes in every way, including by committing tricks and/or a series of lies in order to obtain the victim's banking access code. The modes carried out can be in the form of *Phishing*, *Account take over*, *Share login info*, *Pharming*, and even *Typosquatting*.

¹⁵Noor Rahmad, "*Studi Hukum tentang Kejahatan Penipuan Online*", 110

¹⁶ Article 1 number 16 of the ITE Law

¹⁷ See Article 1 of Bank Indonesia Regulation Number: 11/12/PBI/2009 concerning Electronic Money

¹⁸ See General Explanation No. 2 of Bank Indonesia Regulation Number: 11/12/PBI/2009 concerning Electronic Money

The ITE Law does not specify in detail the use of the above fraud mode. In Chapter VII of the ITE Law, starting from Article 27 to Article 37, it provides regulations on prohibited acts in electronic transactions. For example, in Article 30 paragraph (1), it provides a prohibition for; *any person knowingly and without rights or unlawful access to another Person's Computer and/or Electronic System in any way*. The existence of the phrase "by any means" in this article, according to the author, opens the opportunity to be interpreted as "by any mode" including in this case *Phishing, Account take over, Share login info, and/or Pharming*.

Likewise, the act regulated in Article 30 paragraph (2) again contains the phrase "by any means". The full text of the article reads as follows: *"Every Person intentionally and without rights or unlawfully accesses the Computer and/or Electronic System in any way with the purpose of obtaining Electronic Information and/or Electronic Documents"*.

In contrast to the provisions of Article 31 paragraph (1), it only restrictively regulates the prohibition of intercepting or intercepting Electronic Information and/or Electronic Documents in a Computer and/or certain Electronic System belonging to another Person.

Electronic Information (IE) and/or Electronic Documents (DE) have a broad meaning and understanding, but basically DE is defined as any Electronic Information that is created, transmitted, transmitted, received, or stored, among others, in digital form that can be seen, displayed, and/or heard through a Computer or Electronic System, including but not limited to writing, sounds, images, maps, designs, photos or the like, letters, signs, numbers and so on.¹⁹ Based on this understanding and associated with the existence of electronic money whose recording of every transaction is carried out on electronic media, in the context of the ITE Law, numbers that are information about the value of electronic money as displayed on electronic systems such as *M-banking, platforms* digital wallets, and the like, are included in the scope of the meaning of IE and/or DE. Therefore, every time there is a phrase IE and/or DE in the ITE Law, it can also be interpreted in a general way as information about the value of electronic money in an electronic system. Except for IE and/or DE which has been specifically determined by the ITE Law, such as in Article 27 paragraph (1) regulating IE and/or DE that has content that violates morality, Article 27 paragraph (2) regulating IE and/or DE that has gambling content, Article 27 paragraph (3) regulating IE and/or DE that has insulting and/or defamatory content, and so on

THE MODUS OPERANDI OF THE DEFENDANTS IN THE DECISION NUMBER 274/PID.SUS/2023/PN JKT.SEL

In case Number 274/Pid.Sus/2023/PN Jkt.Sel, the South Jakarta District Court examined and decided 9 (nine) defendants in a separate manner, the nine defendants based on the facts of the trial have their respective roles in committing the crime of "*online fraud*". The role of each of the defendants is basically as follows:²⁰

¹⁹ See Article 1 number 1 and number 4 of the ITE Law

²⁰ See Decision Number 274/Pid.Sus/2023/PN Jkt.Sel, 54-57

1. Defendant I, bought MOD APK (application/*software/package check link* . Apk, Check J&T.Apk Receipt, Package Photos. Apk, etc.) from ANGGA and buy the J&T APK from DR (DPO) for Rp.2,000,000,- (two million rupiah) then place an advertisement for the BI Fast Brimo Application on Instagram, and send it to the BRI account owner through the WhatsApp account, which is obtained from APN, with a profit sharing system of 50% each, and if there is a potential victim who opens/clicks on the ad, then the person will be asked to fill in the Username, password, PIN and OTP, and if the prospective victim does so, the data, in the form of Username, password, PIN and OTP enters the Bot belonging to Defendant I, so that Defendant I can access the victim's mobile banking, and then after obtaining the data, in the form of Username, password, PIN and OTP, Defendant I can make transactions to the victim's account. The number of BRI account owners that Defendant I ANDINI has obtained by phishing *links* to post BI Fast advertisements for the Brimo Application on Instagram is as many as 15 BRI account owners with a total amount of money of around Rp. 250,000,000 (two hundred and fifty million rupiah).
2. Defendant II, sending/transferring the money in the victim's account to other accounts that have been prepared by Defendant I, after Defendant II gets the MOD APK (application/*software/package check link*. Apk, Check J&T.Apk Receipt, Package Photos. Apk, etc.) from ANG, and obtain identity data of potential victims from MAW (DPO) or NAN (DPO).
3. Defendant III, advertised a "*web phishing link*" of BRImo (BRI Mobile) through an *Instagram* account with the mode of "free transfer fees even to other banks" by attaching *the link*, and when the prospective victim clicks on the link, the victim will enter a page that asks the user/victim to register/register then there is a username field and *password*. After the prospective victim fills in *the username* and *password*, the notification will be sent to the *Telegram bot account* that has been installed/ installed on *Defendant III's cellphone*, then *Defendant III logs in to the valid BRImo application by entering the username and password* The victim that Defendant III had obtained through a *telegram bot, which he bought from PINKI* for Rp. 1,500,000,- , and after Defendant III managed to enter the victim's BRImo account, then transferred it to the DANA, OVO and Bank Jago accounts that had been prepared.
4. Defendant IV, checked the victim's balance in the BRIMO application after the victim's username and password and OTP were controlled by Defendant I and Defendant II then Defendant IV reported to Defendant I and Defendant II, and Defendant IV had received a profit of approximately Rp. 41,500,000 (forty-one million five hundred thousand rupiah) and approximately 30 (thirty) BRI Bank accounts with a total of money that was successfully transferred from the victims' accounts approximately Rp. 160,000,000,- (one hundred and sixty million rupiah)
5. Defendant V, advertised a phishing link related to the BI Fast Brimo Application on Instagram @brilayanan1874 and Facebook, and when the prospective victim opens the website link will be directed to fill in the username, password, PIN and OTP code, after the victim fills in the instructions then the victim's data automatically enters Telegram 087839624450 the bot belonging to Defendant V, after the data Defendant V, then the Defendant used it to log in to the victim's BRI MO mobile banking

application and then transferred the contents of the funds in the account to Defendant V's OPPO DANA.

6. Defendant VI sent a website link [https://daftar. Bi.Fast.com](https://daftar.Bi.Fast.com) to the victim through advertisements on two *Instagram* accounts owned by Defendant VI with two *usernames*, namely Bank Bri Assistance and Bank Bri services, and information from advertisements or promos *website link* <https://daftar. Bi.Fast.com> then Defendant VI SENDA gave to the victim was an invitation that "Especially for BRI customers, hurry up and register for Bri.fast with the previous transfer rate of Rp.6,500,- (six thousand five hundred rupiah) per transaction between other banks, now it has been changed to 0% free for every transaction between other banks. Unlimited. Register Now!!", and after the victim is deceived and has clicked on *the website link* that Defendant VI SENDA has advertised, then the victim enters the *Mobile Banking username and password*, then the victim receives the OTP code that comes in via SMS, after that the victim copies the OTP code to the website link <https://daftar. Bi.Fast.com>, then the victim clicks on it, the OTP code immediately enters the *telegram bot* application that Defendant VI has *installed on his cellphone*, and then Defendant VI SENDA successfully *logs in* to the victim's *Mobile Banking* then Defendant VI drains or sends / transfers the money in the victim's account to the Bank Jago and CIMB NIAGA accounts Rahmat (DPO), then Rahmat gave cash to Defendant VI through the intermediary of Defendant VI in accordance with the nominal amount transferred by Defendant VI with a commission discount of 7% for RMT from every transaction made by Defendant VI.
7. Defendant VII, only provided a BTPN Bank account and had disbursed money, transferred money from the victim's account to Defendant VII's account in the BTPN account in exchange for 1% of the amount of money received from Defendant VI.
8. Defendant VIII, made a *direct messenger* via Instagram in the form of a phishing link to offer a change in the normal transaction rate or cheap transaction rate of Bank BRI, if anyone responded, Defendant VIII asked the prospective victim to ask for his Whatsapp number, after being given his WhatsApp number then Terdalwa VIII immediately sent a Phissing Link to change the transaction rate of Bank BRI from normal to cheap rates, After that, Defendant VIII conveyed via Whatsapp message to the prospective victim, if you agree, please click on the link and please fill in the data in the link. After the prospective victim fills in the data in the form of Username and Password, then Defendant VIII goes to the BRI MO application, then Defendant VIII logs in using the Username and Password that Defendant VIII obtains from the Phissing Link and then Defendant VIII logs in and asks for a Verification Code sent by Bank BRI to the prospective victim Defendant VIII as a BRI Bank customer, then after the victim unconsciously provides the Verification Code to Defendant VIII, Defendant VIII uses the Verification Code to Login, and after successfully Logging in Defendant VIII can freely control the Account and can see the Balance of the prospective victim of Defendant VIII, and if there is a balance, Defendant VIII immediately transfers it to another account, and after the money is sent to the RMT account to be withdrawn in cash with a commission of 10% to 15% per withdrawal from the transfer of the victim's account balance.
9. Defendant IX, spread the whastapp broadcast about the info that the suspect remembered the sentence was " *HI BRI FRIENDS, WITH THE CHANGE.....etc* to the

number of the prospective victim, send the BRIMO application link to the number of the prospective victim around 50 (five) tens of mobile phone numbers given by the RAN (DPO) and also look for the number in the sniper whatsapp pro application, if the prospective victim enters the user name and password will automatically enter the OTP code, password and username to the telegram bot installed on the RAN cellphone.

If you pay attention to the actions of the defendants from the description above, you will find more than one type of *modus operandi* used by each defendant according to their role in committing *the* crime of online fraud. The *modus operandi* used by the defendants based on the verdict, as well as related to the legal arrangements contained in the ITE Law, can be grouped as follows :

1. *Phishing*, which is the theft of important information by deceiving the victim into accessing a fake website/page to trap the victim. This mode was used by Defendant I, Defendant III, Defendant V, Defendant VI, Defendant VIII, and Defendant IX. It can be seen from the act of posting advertisements and/or sending directly to BRI account owners through the WhatsApp account related to the change in the BI Fast Brimo Application tariff which turned out to be fake, the Defendants' actions were also carried out in *Pharming Mode*, which is a fraud involving software that takes victims to a fake page where they are invited to enter their data.
2. *Share login info*, which is an effort to get sensitive information from the victim's account such as OTP codes, PINs, and *passwords*. This mode is used by Defendant I, Defendant III, Defendant V, Defendant VI, Defendant VIII as a continuation of the first mode. Prospective victims who open the *Phishing* ads will be asked to fill in their Username, password, PIN and OTP, and if the prospective victims do so, the data, in the form of Username, password, PIN and OTP of BRI Mobile will enter the Defendants' Bot
3. *Account take over*, the sudden takeover of someone else's account. This mode is used by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII after successfully knowing the victim's BRI Mobile Username, password, PIN and OTP by *sharing the login information*, the Defendant freely enters and takes over the victim's BRI mobile account to subsequently transfer the victim's funds to another account that has been prepared by the defendants.

It can be seen that the *modus operandi* used by each Defendant is carried out in stages, some are independent. The use of the mode in stages as carried out by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII. The intention of using the tiered mode is that the defendant uses the *Phishing* and/or *Pharming mode*, *Sharing login info*, until the *account take over* is carried out gradually and independently. Meanwhile, the stand-alone ones, such as the mode used by Defendant II, Defendant III, Defendant IV, where Defendant III, did not participate in the *Phishing/Preaching* mode, and *Share login info*, but only took over the account after the other defendant got the victim's access code. Moreover, Defendant VII has a role that does not fall into the category of the above modes. The actions of Defendant VII were explained by the Panel of Judges in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel only limited to "*providing a BTPN Bank*

account and having disbursed money, transferring money from the victim's account to the account of Defendant VII RANO KARNO in the BTPN account in exchange for 1% of the amount of money received from Defendant VI ..."

As discussed earlier, Chapter VII of the ITE Law has provided regulations on prohibited acts in electronic transactions. In relation to the use of the defendant's mode above, there are several legal rules in the ITE Law that can be applied and have relevance to the use of this mode in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel.

The act of *Pishing* and/or *Pharming* as committed by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII, and Defendant IX by disseminating fictitious BRI Mobile information so that the victim accesses a fake website/page to trap the victim, whose implementation involves software to take the victim to the fake page, is a prohibited act as stipulated in Article 28 paragraph (1) of the ITE Law which reads: "*Every person deliberately and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions*".

The use of the phrase "fake news" among the public is closely related to the spread of *hoaxes*, according to Chazawi, "fake news" is news whose content is not in accordance with the real truth (*materiële waarheid*). It is also explained that 'spreading' means conveying (fake news) to the general public, in this case through the media of telematics convergence.²¹ Regarding 'misleading' has to do with fake news being spread, which can deceive people.

The deceptive nature of the content of fake news that is spread misleads the public, thus causing constitutive consequences in the form of consumer losses in electronic transactions. Then what about the word "consumer contained in Article 28 paragraph (1) of the ITE Law?

According to Anton Hendrik, there is no direct relationship between the ITE Law and Law Number 8 of 1999 concerning Consumer Protection. The Consumer Protection Law further regulates obligations and prohibitions for business actors in order to protect consumer rights.²² The use of the phrase "causing loss" in this Article is a sign that Article 28 paragraph (1) is included in the group of material offenses, namely offenses that focus on the consequences caused.²³

Furthermore, another mode that is also used by Defendant I, Defendant II and Defendant III, Defendant V, Defendant VI, Defendant VIII is *Share login info*. namely to obtain sensitive information from the victim's account such as OTP codes, PINs, and *passwords*. After the potential victim opens the misleading false advertisement, they will be asked to fill in their

²¹ Adami Chazawi and Ardi Ferdian, *Kejahatan Informasi dan Transaksi Elektronik*, (Malang Media: Nusa Creative, 2015) 136.

²² Anton Hendrik Samudra, "Modus Operandi dan Masalah dalam Menangkal Kejahatan Penipuan Online". Ibid. 68

²³ Eddy O.S. Hiariej, *Asas Hukum Pidana, Edisi Revisi*, (Yogyakarta: Cahaya Atma Pustaka, 2016), 136.

username, password, PIN and OTP. Furthermore, if the prospective victim does so, the data, in the form of username, password, PIN and OTP of BRI Mobile enters the *Bot* belonging to the Defendants. The victims who did this were of course due to a trick both from the *phishing link* and from the display in the fake BRI electronic system. In relation to the use of the defendant's mode above, the legal rules in the ITE Law that can be applied and have relevance to the mode used by the Defendants in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel are as stipulated in article 35 of the ITE Law which reads:

"Every Person intentionally and without rights or against the law manipulates, creates, changes, disappears, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if they are authentic data."

Finally, the sudden takeover of other people's accounts, known as *the Account take over mode*, was also carried out by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII by logging in and taking over the BRI mobile accounts belonging to the victims. In relation to the use of the defendant's mode above, the legal rules in the ITE Law that can be applied and have relevance to the mode used by the Defendants in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel are as stipulated in Article 30 paragraph (1) of the ITE Law which reads: *"Every Person intentionally and without rights or unlawfully accesses another Person's Computer and/or Electronic System in any way"*. Related to this arrangement, it is also known as *Illegal Acces*. Even more severe, after committing illegal acces, then the defendant took the victim's money contained in the victim's BRI Mobile electronic system to be subsequently transferred to each defendant's account as prepared. Therefore, the actions of Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII also meet the elements of Article 30 paragraph (2) of the ITE Law which reads: *"Every Person intentionally and without rights or unlawfully in any way transfers or transfers Electronic Information and/or Electronic Documents to the Electronic System of another Person who is not entitled."*

Unlike the other Defendants, Defendant IX only played a role in providing a BTPN Bank account and had disbursed money, transferring money from the victim's account to Defendant VII's account in the BTPN account in exchange for 1% of the amount of money received from Defendant VI. In terms of the Criminal Provisions of Defendant IX's Acts, it is included in "Assistance" as stipulated in Article 56 2 of the Criminal Code which determines: *"Convicted as an accomplice to a crime: ... 2. Those who deliberately provide opportunities, means or to the point of committing crimes."* Exactly helped Defendant VII provide or provide facilities in the form of BTPN accounts in carrying out his actions. The sanction for the "helper" in question, according to the provisions of Article 57 of the Criminal Code paragraph (1), the maximum principal penalty for the crime is reduced by one-third.

Against Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII, who in all their actions use the *Phishing* and/or *Pharming mode*, *Share login info* in stages which leads to the transfer of funds belonging to the victim to each account that has been inserted by the defendant, where each act has its own legal rules. Therefore, in this

section, it is also necessary to review a little about "togetherness" as the teachings of *Concursus idialis* (Article 63 of the Criminal Code), *Concursus realist* (Article 65 of the Criminal Code), and continuing acts (Article 64 of the Criminal Code),

Concursus Idealis, which is the combination of regulations, where from one act carried out by the perpetrator there are several rules that are violated, then *Concursus Realis*, which is the concomitant of deeds, where the perpetrator commits several acts and the acts committed by the perpetrator must be seen as each standalone, the last is the continuous act, where between one act and another act committed by the perpetrator There is a close relationship, so that some of these actions are seen as one act

Regarding this, it has been regulated in Article 65 of the Criminal Code which states:

"In the case of the concomitance of several acts that must be seen as stand-alone acts so that they are several crimes, which are threatened with the same principal crime, then only one crime is imposed".

Regarding the threat of criminal sanctions for the perpetrators, "concurrency is regulated in paragraph (2), namely: *"The maximum penalty imposed is the maximum amount of criminal punishment threatened for the act, but it may be more than the maximum aggravated penalty plus one-third"* ²⁴

The results of previous research conducted by Alif Oksaryan Mulyana, and Diana Lukitasari have concluded as follows:

"Based on the opinions expressed by experts, where the limitation or characteristic of a continuing act itself is from a single intention or based on one criminal intention which is related to "there is such a relationship between the acts committed". Where the deeds committed by the perpetrators are based on or based on one evil intention or what we call one criminal intention" ²⁵

Based on this, the series of modes and acts carried out by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII, can be considered as a continuing act as stipulated in Article 64 of the Criminal Code as follows:

"If between several acts, even though each is a crime or an offense, there is a relationship in such a way that it must be regarded as one continuous act, then only one criminal rule is applied; if it is different, the one applied contains the most severe main criminal threat"

This is also supported by the opinion of Mahrus Ali who said that there are several

²⁴Alif Oksaryan Mulyana, and Diana Lukitasari, "Penerapan Aturan Perilaku Lanjutan dalam Keputusan Perkara Pidana", *Recidive Journal* 11 no 3, (December 2022), 268, <https://doi.org/10.20961/recidive.v11i3.67459>, 267-274

²⁵ *Ibid.* 273 reviews

conditions so that an act can be seen as a continuing act. The conditions in question are:

1. There is a decision of the maker's will, in the sense that a series of several criminal acts that occur must arise from one will or malicious intent
2. Some of the criminal charges committed must be of the same type or at least the same qualifications
3. The time interval between conducting one criminal conversation and another criminal act should not be too long or must not be in a long grace period.²⁶

The essence of a continuing criminal act, according to the Constitutional Court, is that the acts of one and the other are closely interrelated and are a series of manifestations of criminal acts which can then be said to be a criminal act that has a continuing nature²⁷

LAW ENFORCEMENT AGAINST *ONLINE FRAUD* PERPETRATORS BY THE PUBLIC PROSECUTOR AND JUDGE IN DECISION NUMBER 274/PID. SUS/2023/PN JKT. SELL

The Role of Public Prosecutors and Judges in Law Enforcement

Law enforcement aims to improve order and legal certainty in society. This is done by regulating the functions, duties and authorities of agencies responsible in the field of law enforcement in accordance with their respective competencies and based on a good system of cooperation and assistance to achieve goals.²⁸

In law enforcement in Indonesia, there are four important pillars, if one of the law enforcement agencies is tainted by the actions of one of the individuals from the law enforcement agency, then it is certain that the law will not be able to function effectively which can eliminate the public's sense of trust in the law enforcer. The four pillars of law enforcement are judges, prosecutors, police, and advocates.²⁹ Of all the law enforcers mentioned earlier, the only ones that will be discussed further in this article are the Prosecutors and Judges.

In article 1 number 1 of Law No. 16 of 2004 concerning the Prosecutor's Office, it is said:
"The prosecutor is a functional official authorized by law to act as a public prosecutor and

²⁶ Ali, Mahrus, *Dasar-dasar Hukum Pidana*, (East Jakarta: Sinar. Grapika, 2011), 139

²⁷ See the Decision of the Constitutional Court of the Republic of Indonesia Number 84/PUU-XVI/2018 concerning the Constitutionality Testing of Articles 64, 65, and 67 of the Criminal Code

²⁸ Sanyoto, "Law Enforcement in Indonesia", *Journal of Legal Dynamics* 8, no 3, (October, 2007): 119, <https://dinamikahukum.fh.unsoed.ac.id/index.php/IDH/article/view/74/226> 119-204

²⁹ Ali Imron, "Peran dan Kedudukan Empat Pilar dalam Penegakan Hukum Hakim, Kejaksaan, Kepolisian, dan Advokat Terkait dengan Penegakan Hukum dalam Kasus Korupsi" *Jurnal Surya Kencana Dua* 6 no.1, (March, 2016): 92, <http://dx.doi.org/10.32493/jdmhkdmhk.v6i1.340>, 83-107

implementer of court decisions that have obtained permanent legal force and other authorities based on the law".³⁰

The Indonesian Prosecutor's Office is a state institution that exercises state power, especially in prosecution matters. As an institution authorized to enforce law and justice, the Prosecutor's Office is led by the Attorney General who is appointed and responsible to the President. The Attorney General's Office, the High Prosecutor's Office, and the District Attorney's Office are all institutions of state power, especially in the field of prosecution, where everything is an inseparable unit.³¹

Furthermore, in Law No. 48 of 2009 concerning Judicial Power, Article 1 number 5 states:

"Judges are in the Supreme Court and judges in the judicial bodies under it in the general judicial environment, religious environments, military courts, state administrative judicial environments, and judges in special courts in the judicial environment."

The main task of a judge is, of course, in the field of law enforcement and the administration of justice independently and impartially. Judges have the authority to adjudicate and decide cases filed by related parties, including deciding whether someone is guilty or innocent by prioritizing justice and truth.³²

Based on their respective roles and functions, in the next section the author will describe the law enforcement efforts carried out by the Prosecutor, and the judge as reflected in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel.

Indictment and Demands of the Public Prosecutor and Judge's Considerations in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel

The Indictment occupies a central position in the examination of criminal cases in the Court, because the Indictment is the basis and limits the scope of the examination.³³ The indictment is the crown in the trial that must be maintained and maintained steadily by the Public Prosecutor.³⁴

In literature and jurisprudence, it is known that there are several types of indictments. Which form is appropriate to be used in prosecuting a case, cannot be determined as a general benchmark, because the form of indictment will largely depend on the pattern of the criminal act handled by the prosecution. In practice, various types of indictments are

³⁰See Article 1 number 1 of Law Number 16 of 2004 concerning the Prosecutor's Office

³¹ Ali Imron, Ali Imron, "Peran dan Posisi Empat Pilar dalam Penegakan Hukum Hakim, Kejaksaan, Kepolisian, dan Advokat Terkait dengan Penegakan Hukum dalam Kasus Korupsi", 96

³² Indonesian Republic Law No. 48 of 2009, concerning Judicial Power

³³See the Circular Letter of the Attorney General of the Republic of Indonesia Number: SE-004/J.A/11/1993 dated November 16, 1993 concerning the Preparation of Indictments,

³⁴ Nova Aulia Pagar Alam, La Ode Husen, and Kamri Ahmad, "Efektivitas Penyusunan Surat Dakwaan oleh Jaksa Penuntut Umum", *Journal of Lex Generalis* 1, no 6, (November 2020): 913, <https://doi.org/10.52103/ilg.v1i6.236>, 912-927

known. These types of indictments include, Single Indictment, Surat Dakwaan Alternatif, Surat Dakwaan Subsider, Dakwaan Kumulatif, dan Surat Dakwaan Gabungan/Kombinasi.³⁵

In Decision Number 274/Pid.Sus/2023/PN Jkt.Sel, the Indictment submitted by the Public Prosecutor (JPU) is a Joint/Combination Indictment. Based on SEJA No. 004/1993, it is emphasized that in the form of a combined indictment, the cumulative indictment is combined/combined with the alternative indictment or Subsidaire. The emergence of this form is in line with the development in the field of crime which is increasingly varied both in its form/type and in the *modus operandi* used.³⁶ In the Indictment of Case Number 274/Pid.Sus/2023/PN Jkt.Sel, the Public Prosecutor used a combination of alternative indictments and cumulative indictments. Alternative charges are used when certainty has not been obtained about which Criminal Acts are the most appropriate to prove. In alternative indictments, even though the indictment consists of several layers, only one indictment is proven without having to pay attention to the order and if one of them has been proven, then the indictment on the other layer does not need to be proven again. In the form of this indictment, between one layer and the other use the conjunction "*or*".³⁷

On the other hand, according to Rocky Marbun, the form of cumulative indictment is used in relation to what is called *samenloop/concursus* or *deelneming*. Basically, this indictment is used in terms of facing a person who commits several criminal acts or several people who commit one criminal act, strictly speaking, the criminal act charged can be in the form of an independent act, or it can also be a continuing act.

In case Number 274/Pid.Sus/2023/PN Jkt.Sel, the Public Prosecutor has filed an indictment with the use of legal rules as follows:

1. Article 32 paragraph 2 jo Article 48 paragraph 2 of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions jo Article 55 paragraph 1 to 1 of the Criminal Code.; *or second*
2. Article 30 paragraph 2 jo Article 46 paragraph 2 of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions jo Article 55 paragraph 1 to 1 of the Criminal Code; *and second*,
3. Article 3 Jo Article 2 paragraph (1) of Law of the Republic of Indonesia No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes jo Article 55 paragraph 1 to 1 of the Criminal Code

From the formulation of the use of the above legal rules, the prosecutor assessed that at the time the case was submitted to the court, there was no certainty about which Criminal Acts were the most appropriate to prove. This can be seen from the use of Article 32 paragraph (2) jo Article 48 paragraph (2) of the ITE Law with Article 30 paragraph (2) jo Article 46 paragraph 2 of the ITE Law alternatively. On the other hand, the prosecutor has

³⁵ Rocky Marbun, *Telaah Kritis-Filosofis PRAKTIK PERADILAN PIDANA Membongkar Oposisi Biner antara Kekuasaan dan Kewenangan*, (Yogyakarta: CV. Arti Bumi Intaran Mangkuyudan, 2019), 308

³⁶ *Ibid*, 314

³⁷ See the Circular Letter of the Attorney General of the Republic of Indonesia Number: SE-004/J.A/11/1993 dated November 16, 1993 concerning the Preparation of Indictment

believed that the Defendants' actions, in addition to violating one of the rules in the ITE Law above, also violated Article 3 Jo Article 2 paragraph (1) of Law of the Republic of Indonesia No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes. Meanwhile, the use of Article 55 paragraph 1 to 1 of the Criminal Code related to the inclusion contained in each indictment, indicates that of all the defendants, among them there are those who committed, those who ordered to do, and those who participated in committing the acts as charged³⁸

Based on the results of the evidence conducted by the Prosecutor at the trial, the Prosecutor then filed a charge against all the Defendants with a prison sentence of 3 (three) years each reduced while the Defendants were in custody and a fine of Rp. 500,000,000,- (five hundred million rupiah) subsidy of 6 (six) months of imprisonment. This is based on the actions of the Defendants who, according to the prosecutor, violated the first indictment (the first alternative), namely Article 32 paragraph (2) jo Article 48 paragraph 2 of the ITU Law, and Article 3 jo Article 2 paragraph (1) of Law of the Republic of Indonesia No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes jo Article 55 paragraph 1 to 1 of the Criminal Code.³⁹

In the end, the Panel of Judges of the South Jakarta District Court in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel decided that the defendants' actions had been legally and convincingly proven guilty of committing a criminal act, "*...participate in deliberately and without rights or unlawful in any way transferring or transferring electronic information and/or electronic documents to the electronic system of another person who is not entitled*" as in the First Indictment and the crime of "Money Laundering" as in the Second Indictment. On that basis, the Panel of Judges sentenced the Defendants to imprisonment for 3 (three) years each and a fine of Rp.500,000,000,- (five hundred million rupiah) with the provision that if the fine is not paid by the Defendants, it will be replaced with imprisonment for 6 (six) months each. Thus, there is a similarity between the JPU's Demands, and the verdict handed down by the Panel of Judges, both from the use of the rule of law, and the punishment.

If we return to the description of the judge's consideration, where in carrying out his actions, the defendants have different roles. Just like Terakwa IX who only plays a role in providing a BTPN Bank account which is used to transfer money from the victim's account to the account of Defendant VII, normatively, this can be considered as an assistance for a criminal act as stipulated in Article 56 of the 2nd Criminal Code, precisely which provides the means to commit a crime. Furthermore, regarding the criminal threat against "helpers" according to Article 57 paragraph (1) of the Criminal Code, the maximum principal penalty for the crime is reduced by one-third.

Apart from that, in the prosecutor's claim and the judge's verdict, the provisions of Article 3 of the TPPU Law are compact. The use of this Article is certainly related to the judge's

³⁸ See Article 55 paragraph 1 to 1 of the Criminal Code

³⁹. See Decision Number 274/Pid.Sus/2023/PN Jkt.Sel, 5

consideration in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel which states: *"That the Defendants sent the proceeds of crime to the prepared account"*.⁴⁰

If you look closely at the word or element of "transferring" is also found in the provisions of Article 32 paragraph (2) of the ITE Law, the difference is that the object of "transfer" in the ITE Law is *"... Electronic Information and/or Electronic Documents to the Electronic System of other persons who are not entitled"*. Seeing the judge's consideration in determining the defendant's actions to meet the elements of article 32 paragraph (2), as well as to the defendant's actions after successfully logging in to the victim's Mobile Banking, Defendant VI drained or send/transferred money to the account that had been prepared (bang Jago, OVO, DANA, and so on).

As previously described, electronic money contained in an electronic system such as *M-banking*, digital wallet platforms, and the like, is included in the scope of IE and/or DE definition. Meanwhile, *M-banking*, a digital wallet platform (OVO/DANA) is part of the electronic system according to the ITE Law. Up to here, of course, it can be seen that there is a "similarity" between Article 32 paragraph (2) and Article 3 of the TPPU Law, especially related to the "object of transfer". To answer this, based on the principle *of lex specialis derogat legi generali* which is normatively regulated in the provisions of Article 63 paragraph (2) of the Criminal Code, which gives a mandate in the event of an act, which is included in a general criminal rule, is also regulated in a special criminal rule, then only the special one is imposed. Based on that, according to the author, Article 32 paragraph (2) and Article 3 of the Anti-Money Laundering Law cannot be applied simultaneously as long as it concerns the act of "transferring IE and/or DE in the form of electronic money to other electronic systems that are not entitled".

In the event of a conflict of norms as above, the *lex specialist* is the TPPU Law, considering that transactions involving electronic systems are related to Financial Transactions. This is as explained in Article 1 number 4 of the TPPU Law which reads:

"Financial Transaction is a Transaction to make or receive a placement, deposit, withdrawal, bookkeeping, transfer, payment, grant, donation, custody, and/or exchange of a sum of money or other actions and/or activities related to money"

In addition, judging from the application of the law, according to the author, there is a fairly fundamental inconsistency in the indictment of the JPU, precisely whether the series of acts of the Defendant is included in *the Realist Concursus* (Article 65 of the Criminal Code), or whether the act continues (*Article 64 of the Criminal Code*). If we look at the facts of the trial, it has been proven that the actions of Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, and Defendant VIII, were based on a series of several acts

⁴⁰This consideration is part of the consideration of the element of "placed, transferred, transferred, spent, paid, granted, deposited, taken abroad, changed form, exchanged for currency or securities or other acts of *Wealth which he knows or should suspect is the result of a criminal act as intended in Article 2 paragraph (1) with the purpose of concealing or disguising the origin of the Property*", see Decision Number 274/Pid.Sus/2023/PN Jkt.Sel, 62

arising from one will, and the time between each series of actions, was carried out so quickly. Based on that, the defendant's actions should be included in the category of Continuing acts that cause legal consequences, only one criminal rule is applied, if it is different, then what is applied is the rule that contains the most severe main criminal threat. In this case, Article 3 of the Anti-Money Laundering Law contains criminal threats imprisonment for a maximum of 20 (twenty) years and a maximum fine of Rp10,000,000,000.00 (ten billion rupiah).

If the construction of the *realist Concursus* doctrine is used as stipulated in Article 65 of the Criminal Code, then each of the Defendant's actions which is also a stand-alone criminal act should also be included in the cumulative indictment. The acts in question include:

1. The act of *Pishing* and/or *Pharming* as committed by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII, and Defendant IX by disseminating fictitious BRI Mobile information so that the victim accesses a fake website/page to trap the victim, whose implementation involves software to take the victim to the fake page, is a prohibited act as stipulated in Article 28 paragraph (1) of the ITE Law which reads: *"Everyone deliberately and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions"*
2. *Share login info* as used by Defendant I, Defendant II and Defendant III, Defendant V, Defendant VI, Defendant VIII are. get sensitive information from the victim's account such as OTP code, PIN, and *password* After the prospective victim opens the "bohog" advertisement, he will be asked to fill in the Username, password, PIN and OTP, and if the prospective victim does so, the data, in the form of Username, password, PIN and OTP of BRI Mobile enters the Bot belonging to the Defendants. The victims who did this were of course due to a trick both from the link and from the display in the fake BRI electronic system. In relation to the use of the defendant's mode above, the legal rules in the ITE Law that can be applied and have relevance to the mode used by the Defendants in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel are as stipulated in article 35 of the ITE Law which reads:

"Every Person intentionally and without rights or against the law manipulates, creates, changes, disappears, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if they are authentic data."

3. Finally, the sudden takeover of other people's accounts, known as *Account take over*, was also carried out by Defendant I, Defendant II, Defendant III, Defendant IV, Defendant VI, Defendant VIII by entering and taking over the BRI mobile accounts belonging to the victims. In relation to the use of the defendant's mode above, the legal rules in the ITE Law that can be applied and have relevance to the mode used by the Defendants in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel are as stipulated in Article 30 paragraph (1) of the ITE Law which reads: *"Every Person intentionally and without rights or unlawfully accesses another Person's Computer and/or Electronic System in any way"*.

One thing that is also quite of concern to the author is related to the non-use of Article 36 *Juncto* Article 51 paragraph (2) of the ITU Law as a criminal burden for the actions of the Defendants, considering that if you pay attention to the consequences of the defendant's actions that have an impact on material losses to the victims, it has fulfilled the elements of Article 36 of the ITE Law which *reads*:

"Every Person deliberately and without rights or against the law commits an act as referred to in Articles 27 to 34 that result in losses to others". Article 51 paragraph (2) of the ITU Law reads: "Every person who meets the elements as referred to in Article 36 shall be sentenced to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiah)".

Meanwhile, for the Judge in deciding a case, even though he has freedom, however, according to Article 182 paragraph (3) of the Criminal Procedure Code, the benchmark in determining the defendant's guilt is in the Indictment.

4. Conclusion

- a. In general, there are many modes of digital fraud, including *Phishing, Scam, Account take over, Social engineering, Share login info, Share card info, ID theft, Typosquatting, Pharming, Skimming, Malware, Lottery Scams, Video Scams, and Scareware*. Among the modes mentioned above, there are several that based on the provisions of the ITU Law are seen as stand-alone criminal acts, such as *Phishing, Pharming, Account take over, Share login info, Pharming, and Skimming*. The Operandi mode used by the Defendants in Decision Number 274/Pid.Sus/2023/PN Jkt.Sel is not all the same, Defendant I, Defendant II, Defendant III, Defendant IV, Defendant V, Defendant VI, Defendant VIII, and Defendant IX use the *Pishing and/or Pharming mode, Share login info, and Account take over*. Meanwhile, Defendant VII only played the role of a person who helped provide the means of providing a bank account for Defendant VI. Law enforcement is aimed at improving order and legal certainty in society, the law enforcers discussed in this article are as by the Prosecutor and the Judge who examined and decided Case Number 274/Pid.Sus/2023/PN Jkt.Sel. Based on the results of the evidence carried out by the JPU. Furthermore, the Public Prosecutor filed charges against all Defendants with imprisonment for 3 (three) years each, and a fine of Rp. 500,000,000,- (five hundred million rupiah) subsidy of 6 (six) months of imprisonment. This is based on the actions of the Defendants who, according to the prosecutor, violated the first indictment (the first alternative), namely Article 32 paragraph (2) jo Article 48 paragraph 2 of the ITU Law, *and* Article 3 jo Article 2 paragraph (1) of Law of the Republic of Indonesia No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes jo Article 55 paragraph 1 to 1 of the Criminal Code. Finally, the Panel of Judges handed down the verdict according to the JPU Directive.
- b. The sentence handed down was relatively light for Defendant I, Defendant II, Defendant III, Defendant IV, Defendant V, Defendant VI, Defendant VIII, and Defendant

IX, considering that the maximum criminal threat in Article 3 of the Anti-Corruption Law is 20 years. Moreover, in this case, it is proven that the occurrence of *a realist Concursus* is concurrent with an act as stipulated in Article 32 paragraph (2) jo Article 48 paragraph 2 of the ITU Law. Legally, the threat of imprisonment against the defendants is the heaviest plus one-third. Except for Defendant VII who is only an "assistant" of Defendant VI. In addition, the author finds that there is a fairly basic inconsistency in the indictment of the JPU, where the entire series of Defendant's Acts should be assessed as a continuing act, not a concurrent. However, even if the acts of Defendant I, Defendant II, Defendant III, Defendant IV, Defendant V, Defendant VI, Defendant VIII, and Defendant IX can be seen as concurrent, other acts should also be included, namely *Pishing* and/or *Pharming*, *Sharing login info*, and *Account take over* as an article that is charged cumulatively. Finally, the author sees other non-seriousness carried out by the prosecutor in the case. This can be seen from the non-inclusion of Article 36 of the ITE Law as a "burden", stinging, the Defendant's actions have clearly harmed his victims.

References

- Alam, Nova Aulia Pagar, La Ode Husen, dan Kamri Ahmad, "Efektivitas Penyusunan Surat Dakwaan Oleh Penuntut Umum", *Journal of Lex Generalis* 1, no 6, (Nopember 2020): 913, <https://doi.org/10.52103/jlg.v1i6.236>, 912-927
- Ali, Mahrus, *Dasar-Dasar Hukum Pidana*, (Jakarta Timur: Sinar. Grafika, 2011
- Chazawi, Adami dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik, Media*. Malang: Nusa Creative, 2015
- Dirjosisworo, *Ruang Lingkup Kriminalogi*, Jakarta, Rajawali, 1984
- Fajar, Mukti ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Penelitian Hukum Empiris*. Yogyakarta: Pustaka Pelajar, 2010
- Hiariej, Eddy O.S, *Prinsip-Prinsip Hukum Pidana, Edisi Revisi*, Yogyakarta: Cahaya Atma Pustaka, 2016
- Imron, Ali, "Peran Dan Kedudukan Empat Pilar Dalam Penegakan Hukum Hakim Jaksa Polisi Serta Advokat Dihubungkan Dengan Penegakan Hukum Pada Kasus Korupsi" *Jurnal Surya Kencana* Dua 6 no.1, (Maret, 2016): 92, <http://dx.doi.org/10.32493/jdmhkdmmhk.v6i1.340>, 83-107
- Kansil, C.S.T., *Ilmu Negara Umum dan Indonesia*. Jakarta : PT Pradnya Paramita, 2001
- Kitab Undang-Undang Hukum Pidana
- Kurnia, Novi, *et al* , *Penipuan Digital Di Indonesia: Modus, Medium, Dan Rekomendasi*. Jogjakarta : Program Studi Magister Ilmu Komunikasi Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gadjah Mada, 2022
- Marbun, Rocky, *Telaah Kritis-Filosofis Praktik Peradilan Pidana Membongkar Oposisi Biner antara Kekuasaan dan Kewenangan*. Yogyakarta: CV. Arti Bumi Intaran Mangkuyudan, 2019
- Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana, 2013
- Muladi, Lilik, *Seraut Wajah Putusan Hakim: Studi Kasus Prita Mulyasari*, Jakarta : Rineka Cipta, 2009
- Mulyana, Alif Oksaryan, dan Diana Lukitasari, "Penerapan Aturan Perbuatan Berlanjut Dalam Putusan Perkara Pidana", *Jurnal Recidive* 11 no 3, (Desember 2022), 267-274. <https://doi.org/10.20961/recidive.v11i3.67459>
- Moeljatno, *Asas-Asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2015
- Peraturan Bank Indonesia Nomor: 11/12/PBI/2009 Tentang Uang Elektronik (*Electronic Money*)

- Putusan Mahkamah Konstitusi Republik Indonesia Nomor 84/PUU-XVI/2018 mengenai Pengujian Pasal 64, 65, dan 67 KUHP terhadap Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, 31 Oktober 2018
- Putusan Pengadilan Negeri Jakarta Selatan Nomor 274/Pid.Sus/2023/PN Jkt.Sel, perihal Kasus Penipuan Online Terdakwa II – Terdakwa IX
- Rahmad, Noor, "Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online", Jurnal Hukum Ekonomi Syariah 3 no 2, (April 2019): 103-117. <https://doi.org/10.26618/j-hes.v3i2.2419>
- Samudra, Anton Hendrik, "Modus Operandi Dan Problematika Penanggulangan Tindak Pidana Penipuan Daring", Jurnal Mimbar Hukum 31 no. 1, (2019), 59-74. <https://doi.org/10.22146/jmh.34786>.
- Sudoyo, Wahyu, "Catatan Kominfo, Korban Penipuan Online Capai 130 Ribu pada 2022", <https://infopublik.id/kategori/nasional-sosial-budaya/715547/catatan-kominfo-korban-penipuan-online-capai-130-ribu-pada-2022>, (diakses 2 Januari 2023)
- Sanyoto, "Penegakan Hukum Di Indonesia", Jurnal dinamika hukum 8, no 3,(Oktober, 2007):119-204, <https://dinamikahukum.fh.unsoed.ac.id/index.php/JDH/article/view/74/226>
- Surat Edaran Jaksa Agung Republik Indonesia Nomor: SE-004/J.A/11/1993 Tanggal 16 Nopember 1993 Tentang Pembuatan Surat Dakwaan
- Undan-Undang Nomor 48 tahun 2009, tentang Kekuasaan Kehakiman
- Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan
- Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
- Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008