Juridical Review of Taking Customer Funds Without Rights Through Electronic Transactions: Study Decision Number 592/Pid.sus/2019/Pn/Jkt.Brt

Desy Yurita Siregar and Januar Agung Saputera
Universitas 17 Agustus 1945 Jakarta, Indonesia

Keywords: Electronic Transactions, Banking, Application of Sanctions, Legal Protection.

Abstract: The use of technology and information has now been widely used by people individually and by institutions. The result of advances and developments in information and communication technology that has the greatest influence is on financial institutions (banking). The use of the internet by financial institutions or banks which is now known as internet banking, in addition to providing convenience for customers, internet banking can also have a negative impact on each of its users, one form of such crime is the breach of customer accounts by taking customer funds without rights carried out by unauthorized individuals.the purpose of this study carried out is to find out how to apply sanctions Criminal against the case study of judgment number 592/Pid.sus/2019/Pn/Jkt.Brt relating to the unauthorized taking of funds through electronic transactions when reviewed from the ITE Law and the Criminal Code and How the legal protection provided by banks to customers as victims of theft of customer funds through mobile banking as a means.then the type of research used is normative juridical research (literature studies) with data sources obtained from primary, secondary and tertiary legal materials, then the type of approach taken is the type of statutory approach (Statute Approach). so that it can be concluded that for the application of criminal sanctions for taking customer funds without rights through electronic transactions, criminal sanctions or administrative sanctions can be imposed in accordance with Article 35 jo Article 51 paragraph (1) jo Article 30 jo article 32 jo Article 46 paragraph (1) of Law of the Republic of Indonesia 11 of 2008 concerning ITE as amended into Law Number 19 of 2016 concerning electronic information and transactions jo Article 363 of the Criminal Code jo Article 263 of the Criminal Code.

1 INTRODUCTION

1.1 Background

Technological developments in the current era of globalization have brought real changes to humans in all corners of the world for our own country (Indonesia). As technology continues to permeate more aspects of daily life and internet usage expands globally, the variety of criminal activities originating within the digital realm will inevitably proliferate in kind. In the world of banking, various new innovations have also been presented in improving services and wanting to provide convenience. in making transactions for each customer. Meanwhile, one form of service provided is internet banking facilities. The presence of internet banking is a type of banking service that is widely used by everyone currently. While this service does exist, its presence does not preclude diverse alternatives from potentially arising. forms of crime in the banking world.

One type of crime in the banking world that will be studied is the unauthorized taking of customer funds through electronic transactions, where this crime was committed by several perpetrators such as Mr. Daniel Iskandar as the defendant and together with other colleagues who simultaneously controlled or controlled customer funds in full, so with the background of the problem above, the author wants to conduct research on the cases that occurred, so this research is entitled **"Judicial Review of Unauthorized Taking of Customer Funds Through Electronic Transactions (Decision Study Number 592 /Pid.sus/2019 /Pn/Jkt.Brt).**

Siregar, D. and Saputera, J.
Juridical Review of Taking Customer Funds Without Rights Through Electronic Transactions: Study Decision Number 592/Pid.sus/2019/Pn/Jkt.Brt.
DOI: 10.5220/0012583000003821

In *Proceedings of the 4th International Seminar and Call for Paper (ISCP UTA '45 JAKARTA 2023)*, pages 505-511
ISBN: 978-989-758-691-0; ISSN: 2828-853X

2 PROBLEM FORMULATION

Based on the explanation described above, the issues that surface are:

1. How are criminal sanctions applied to the case study of Decision Number 592/Pid.sus /2019/Pn/Jkt.Brt relating to unauthorized withdrawal of funds through electronic transactions when viewed from the ITE Law and the Criminal Code?
2. What is the legal protection provided by the bank to customers who are victims of theft of customer funds through mobile banking as a means?

3 RESEARCH METHODS

The type of research used in this case is normative juridical research, namely by examining library materials or secondary data as basic material or studies in this research. Where the law in statutory regulations is used as a benchmark or consideration in analyzing each case that occurs, then normative juridical places law as a building system of norms, principles, rules of statutory regulations, court decisions, agreements and doctrines or expert opinions. then the type of approach used is the statutory approach (statute approach) which is needed to further study of the applicable legal basis, as well as a legislative approach is carried out by examining all laws and regulations relating to legal issues that are relevant to the legal issue being researched.

3.1 Research Specifications

The definition of the descriptive analytical method (Sugiono: 2009) is a method that functions to describe or provide an overview of the object being studied through data or samples that have been collected as they are without carrying out analysis and drawing general conclusions

3.2 Data Source

The data source in this research is secondary data, namely data obtained through library materials by collecting from various reading sources that are relevant to the problem being researched, namely by carrying out a series of activities in the form of reading, quoting from books, documents, and legal literature. related to the problem under study.

3.3 Data Collection Techniques

Literature study is all efforts made by researchers to collect information that is relevant to the topic being researched. This information can be obtained from books, articles, journals, previous research,

3.4 Theory Review

The theories used are identification which can be used as a basis for thinking for carrying out research or in other words to describe the frame of reference or theory used to study problems. Because the problem being discussed is a Juridical Review of Unauthorized Taking of Customer Funds Through Electronic Transactions (Case Study Decision Number: 592 /Pid.sus /2019/Pn/Jkt.Brt), several theories are presented below, including:

1. Sentencing Theory

The aim of the theory of punishment is to:

a. "Guiding convicts to repent and become virtuous and useful members of society."
b. "Remove the stains caused by criminal acts."
c. "Punishment is not intended to cause suffering and is not permitted to degrade human dignity."
d. "Provide a deterrent effect on perpetrators of criminal acts so that they do not repeat their actions."

2. Legal Protection Theory

A protection provided to legal subjects in the form of legal instruments, both preventive and repressive, both written and unwritten. In other words, legal protection is an illustration of the function of law, namely the concept where law can provide justice, order, certainty, benefit, and peace.

3. Law Enforcement Theory

Law enforcement is carried out with the aim of realizing a sense of justice, legal certainty, and benefits for the community, especially perpetrators of criminal acts, so that they can provide legal protection, create a sense of security and achieve a more peaceful life within the community.

4. Theory of Criminal Responsibility

The concept of criminal responsibility does not only concern legal matters but also concerns moral values or general decency adhered to by a society or groups in society. This is done so that criminal liability is achieved by fulfilling justice. (Rusmana, SH, 2006).

3.5 Analysis and Discussion

3.5.1 Chronology of Case Study Decision Number 592/Pid.sus/2019/Pn/Jkt.Brt

The chronology of this case began on Wednesday, May 22 2019, where the West Jakarta District Court had the authority to examine and try this case with the defendant, Mr Daniel Iskandar, along with other colleagues. who sell customer data using the financial information reporting system (SLIK) of the financial services authority (OJK) which contains the NIK KTP, complete address of the customer, address of work place, registered with any bank, number of credit card limits, current or not credit card payments, the data was sold for IDR 100,000 (One Hundred Thousand Rupiah) per data. After obtaining the customer data, the perpetrators launched a crime starting with the victim named Mr. Ilham Bintang.

The perpetrator tried to contact Mr. Ilham Bintang's telephone number but could not be contacted because Mr. Ilham Bintang was in Australia. Next, another suspect made a Subscriber Identity Module for mobile or a new SIM card to get a duplicate of Mr. Ilham Bintang's telephone number by using a fake KTP in the name of Mr. Ilham. Bintang at the Indosat outlet in the shopping center in the Bintaro area. The fake ID card was made by one of the female perpetrators with the initials TR in Jakarta for IDR 1,250,000 (One million two hundred and fifty thousand rupiah), then the ID card was made At the request of perpetrator TR and perpetrator W, the fake data and images (in separate files) sent by perpetrator D alias E were handed over again to be made to the perpetrator with the initials JW in the area of Jl. Ciputat Raya No. 4, Pondok Pinang, Jakarta - South with costs Rp. 300,000,- (Three hundred thousand rupiah).

The syndicate of perpetrators then shared the task of handing over Mr. Ilham Bintang's duplicate number to other perpetrators to then break into the account by hacking his personal e- mail account then entering the Yahoo application to find out Mr. Ilham Bintang's personal e-mail because it required a password to open it. When asked to reset (To open Mr. Ilham Bintang's e- mail, an OTP (One Time Password) was sent to the new telephone number. So, that was used as data to change the password (Br Ilham Bintang's personal e-mail).

Then after the e-mail was opened, the bank data was opened, so (Mr. Ilham Bintang's) account was completely drained, because of this there was an unknown transaction used on Mr. Ilham Bintang's BNI Bank credit card by the perpetrator by making purchases at LAZADA in the form of Vouchers. gold amounting to Rp. 8,500,000,- (eight million five hundred thousand rupiah) for 10 transactions totaling Rp. 85,000,000,- (eighty five million rupiah) after successfully spending the gold Voucher then Redeeming the Voucher to the Pluang account becomes After the Gold became Gold, the Gold was bought for Rp. 85,000,000,- (Eighty-five million rupiah) which was then resold by one of the perpetrators with the initials E on the Pluang application for Rp. 83,000,000,- (Eighty-three million rupiah) within 2 (two) days the Pluang application transferred Rp. 83,000,000,- (Eighty-three million rupiah), to the Bank Sumsel Babel account in the name of the perpetrator with the initials AT in the amount of Rp. 37,000,000,- (Thirty seven million rupiah) and to the BCA account of the perpetrator with the initials NM amounting to Rp. 46,000,000,- (Forty-six million rupiah), while on Mr. Ilham Bintang's M-Banking Commonwealth Bank ID, a savings balance of approximately Rp. 255,124,666 was seen. ,- (Two hundred fifty-five million one hundred twenty-four thousand six hundred and sixty-six rupiah) at that time the balance of the money savings had been used by the perpetrator, stealing money through Commonwealth Bank accounts and BNI Bank credit cards totaling IDR 385,000 ,000 (three hundred and eighty-five million rupiah), the perpetrator carried out this operation by transferring transfers to other perpetrator syndicates using various banks.

So according to Mr. Ilham Bintang, the losses in the 2 (two) Commonwealth Bank accounts and the BNI 46 Bank Credit Card were: Savings account amounting to Rp. 61,405,491,- (Sixty one million four hundred five thousand four hundred and ninety one rupiah), Australian Dollar savings account amounting to AUD.25,263 (Twenty five thousand two hundred and sixty three Australian dollars) and BNI Bank Credit Card 46 amounting to Rp.85,000,000,- (Eighty five million rupiah).

The five defendants who underwent trial with split cases included Desar (20), Teti Rosmiawati (46), Wasno (52), Amran Yunianto (53), and Pegik (28). Based on the evidence and facts obtained during the trial, the defendant has been legally and convincingly proven to have committed a crime, namely taking customer funds by breaking into customer accounts/hacking customer data, attempting to break into credit cards, hacking or hacking telephones. , as well as falsifying identity/KTP so that the panel of judges imposed criminal sanctions in accordance with Article 35 in conjunction with Article 51 paragraph (1) in conjunction with Article 30 in conjunction with

Article 46 paragraph (1) of Law Number 11 of 2008 which has been amended to Law Number
19 of 2008 2016 Regarding information and Electronic Transactions in conjunction with Article 363 of the Criminal Code in conjunction with Article 263 of the Criminal Code, namely:

1. "States that the Defendant Daniel Iskandar deliberately and without right or against the law manipulated electronic documents/broke into customer accounts with the aim of obtaining information and/or electronic documents as in the first alternative indictment."
2. "Sentence the Defendant to prison for 10 (ten) years."
3. "Determining that the period of arrest and detention that has been served by the Defendant shall be deducted entirely from the sentence imposed."
4. "Determine that the defendant remains in detention."
5. "Charge the Defendant a case fee of IDR 2,000 (Two Thousand Rupiah).

3.5.2 Consideration of the Panel of Judges in Imposing Criminal Sanctions Based on Case Chronology

In giving a decision on a case, analysis is needed to achieve a fair and appropriate decision so that the analysis used can make it easier to resolve a case. Where this analysis is divided into 2 (two) types, namely the first by analyzing the formal requirements, namely the use and fulfillment of all evidence, the process of carrying out the trial and giving the defendant the rights to have legal representation or present all defenses before the trial. then the second is the material requirements, namely analyzing the accuracy of the accusations and/or demands regarding the defendant's actions as well as the accuracy of the judge's considerations and decision.

1. Formal Requirements In deciding this case, the Panel of Judges must first consider all evidence in accordance with the applicable legal regulations or provisions contained in Article 184 of the Criminal Procedure Code, namely witness statements, expert testimony, evidence contained in the decision and the defendant's statement as well as additional evidence. in the form of electronic information and/or electronic documents.
2. Material Requirements (regarding the accuracy of the accusations and demands with the defendant's actions, as well as the accuracy of the Judge's considerations before deciding the case). The judge's considerations in imposing the severity of the criminal sanctions imposed on the defendant for the crime of manipulating electronic information must consider the background and reasons why the defendant committed the crime. Apart from that, based on the examination at trial, it was not proven that there were factors which eliminated the Defendant's guilt, namely in the form of justification or excuse reasons, and there were also no factors which eradicated the unlawful nature of the Defendant's actions, as a result the Defendant must be responsible for his actions and the Defendant must sentenced to crime.

3.5.3 Legal Protection Provided by Banks to Customers who Are Victims of Theft of Customer Funds Through Mobile Banking as a Means

According to (Satjito Rahardjo) legal protection is an effort to protect a person's interests by allocating a Human Rights authority to him to act in the context of his interests. Then according to (Setiono) legal protection is an action or effort to protect society from arbitrary actions by the authorities which is not in accordance with the rule of law, to create order and tranquility so as to enable humans to enjoy their dignity as human beings.

Customer protection in banking is currently a problem that has not yet found a good position or place in resolving all problems in the national banking system. (Jovinda Ganda, n.d.) where in reality many bank customers are always considered to be in a weak position and do not benefit if problems occur. between customers and business actors, namely the bank itself, so that it can be concluded that customers are victims of every crime that occurs or can be called the injured party. (Annisa & Pradani, n.d.).

Legal protection must be guaranteed and given to everyone, because it is part of human rights and this has been regulated by law, this protection is also inseparable from all bank customers who have experienced a form of criminal act/crime either conventionally or through internet network (mobile banking). (Suhariyanto et al., 2016).

Legal protection for customers can be carried out in 2 forms, namely (Ni et al., n.d.): firstly, there is indirect protection, meaning that all risks of loss experienced by victims/customers are caused by the existence of a policy or from the activities of the bank.(in article 29 paragraphs (2,3 and 4) in conjunction with article 11, article 34 paragraphs (1,2

and 3), in conjunction with article 35 of Law No.10 of 1998 concerning Banking, then the second is with direct protection in the sense that the risks that occur are due to all the mistakes of the bank (Presidential Decree No.26 of 1998 concerning Guarantees for Commercial Bank Liabilities, article 37 B paragraph (1), (2), Law No.10 of 1998 concerning Banking). (Hermansyah, 2009).

According to (Marulak; Padede) protection of bank customer data in Indonesia can be done in 2 (two) ways, namely:

A. Implicit deposit protection, namely protection resulting from effective bank supervision and guidance, which can prevent bank bankruptcy. This protection can be obtained through, (Budi Fitriadi, 2000). Among others

(1) Legislative regulations in the banking sector, namely the rules or codes governing banking.

(2) Protection resulting from effective supervision and guidance, carried out by Bank Indonesia, supervising bank performance in protecting customers who save funds and providing guidance for those who are unhealthy.

(3) Efforts to maintain the business continuity of the bank as an institution in particular and protect the banking system in general,

(4) Maintaining the bank's health level, namely by coaching carried out by Bank Indonesia.

(5) Carrying out business in accordance with the prudential principle, the provisions of Article 2 of Law Number 10 of 1998 stipulate that Indonesian Banking carries out its business based on Economic Democracy using the prudential principle. From this provision, it shows that the principle of prudence is one of the most important principles that must be applied or implemented by banks in carrying out their business activities.

(6) Methods of providing credit that do not harm the bank and the interests of customers, and

(7) Providing risk information to bank customers.

B. Explicit deposit protection, namely protection through the establishment of an institution that guarantees public savings, so that if a bank fails, this institution will replace public funds deposited with the failed bank. This protection is obtained through the establishment of institutions that guarantee public savings, as regulated in Presidential Decree of the Republic of Indonesia Number. 26 of 1998 concerning Guarantees for Commercial Bank Liabilities. 3 Law Number 10 of 1998 concerning Banking mandates the establishment of a Deposit Guarantee Institution (LPS) as the implementer of guarantees for public funds.

Then there are several aspects of computer security system protection that are important for banks to protect, namely:

a. Privacy and Confidentiality

The most important thing in this aspect is efforts to protect data and information from parties who are not allowed to access it. Privacy refers more to data that is private. For example, user emails that admins are not allowed to read. Meanwhile, confidentiality relates to data given to a party for a certain matter and is only permitted for that matter. For example, an ISP's customer list.

b. Integrity

This aspect prioritizes that data or information must not be accessed without the owner's permission. For example, an email sent by the sender should not be able to be read by anyone else before it reaches its destination.

c. Authentication

This emphasizes the authenticity of data or information, including the party who provided the data or accessed it. Examples include using a PIN or password.

d. Availability

Aspects related to the availability of information when needed. An information system that is attacked can hamper the availability of the information provided.

e. Access Control

This aspect relates to how to access information. This is usually related to data classification (public, private confidential, top secret) & user (guest, admin, top manager, etc.), authentication mechanisms and privacy. Often done by using a combination of user ID or password with other methods with cards.

f. Non-Repudiation

This emphasizes that a party cannot deny having carried out a transaction or accessed certain data. This aspect is very important when it comes to e-commerce. For example, someone who sends an email ordering goods cannot be denied having sent that email. However, even though the bank has provided security aspects as explained, there are still risks associated with carrying out internet banking activities, including theft of bank customer funds. Through the internet.

Based on the case study that occurred, according to the author's observations, the imposition of criminal sanctions against the defendant is still very light, namely 10 (Ten) years in prison, even though it is still very possible to impose sanctions of more than 10 (Ten) years in prison because of his actions not only materially detrimental, but if there is immaterial loss, that is, it can disturb the public, then the panel of

judges really needs to impose administrative sanctions, namely in the form of returning customer funds to the victim or freezing all the proceeds of the crime or confiscating all the defendant's belongings obtained from the proceeds of the crime. Then, banks as business actors are expected to be able to improve their security systems so that this can minimize the forms of crime that occur.

4 CONCLUSION

1. The application of criminal sanctions against people who commit a crime, especially in taking/withdrawing customer funds without the customer's property rights. If viewed from the ITE law, it does not mention specific criminal sanctions but only includes a comprehensive or comprehensive definition, namely each person and their actions. who violates all the rules or elements in the law, then every person, whether individual, group or corporation who is a legal subject can be held accountable so that it is very possible to obtain criminal sanctions. So based on the decision of the Panel of Judges which has obtained permanent legal force (Inkracht) for case study decision Number 592/Pid.sus/2019/Pn/Jkt.Brt. The defendant has been legally and convincingly proven to have manipulated electronic documents, namely by breaking into customer accounts/hacking all customer data so that the panel of judges handed down a decision in accordance with Article 35 in conjunction with Article 51 paragraph (1) in conjunction with Article 30 in conjunction with Article 46 paragraph (1) Law Number 11 of 2008 which has been amended to become Law Number 19 of 2016 concerning Information and Electronic Transactions in conjunction with Article 363 of the Criminal Code in conjunction with Article 263 of the Criminal Code with a prison sentence of 10 years.

2. In order to maintain security factors and legal protection for customers, the government established a law that can provide legal protection and certainty in the operation of electronic systems, namely Law Number 11 of 2008 which has been amended to become Law Number 19 of 2016 concerning Information and Electronic Transactions. Article 15 paragraph

(1) of the ITE Law states that, "every electronic operator must operate an electronic system reliably and safely and be responsible for the operation of the electronic system as it should be. Apart from the legal umbrella above, there are other legal rules that can be used as a legal basis. and in accordance with the principles, functions and objectives of Indonesian banking as stated in Article 2 of Law no. 7 of 1992 as amended by Law no. 10 of 1998 concerning Banking, that "Banks carry out their business on the basis of economic democracy using the principle of prudence.

REFERENCES

Journal

Third Parties: The Case of Fintech "Peer to Peer Lending".

Astrini, D. A. (2015). Legal Protection for Bank Customers Using Internet Banking from Cybercrime Threats. Lex Privatum, 3(1), 149–160

Cynthia, H., 2018, "Personal Data Registration Through Prepaid Cards in Human Rights Perspective", Human Rights Journal, Vol.9, No.2.

Irwan Sugiarto, Silk Day is Celebrated. (2020). Consumers Spiritual Rights in Indonesia: A Legal Study Of Sharia Fintech Implementation In The Consumers Protection Perspective. Ius Journal of Law and Justice Studies, Vol 8, No 3.

Jovin Ganda Ramdhan and Sumiyati, Legal Protection for Customers Skimming Victims Judging from the Law Law Number 8 of 1999, Volume 12. No. 1 p 89

Master of Law Journal, responsibility banking crime through skimming modus operandi Volume7|Number 1| March 2020 Page 37

Lex Privatum Concerning Legal Protection To User Bank Customers Internet Banking From Threats Cybercrime Vol.III/No.1/pg 149

Manulang, Sitohang. (2017). Criminal Liability for Perpetrators of the Crime of Forgery of Documents Belonging to Others For Online Loans (Study Decision Number 871/PID.SUS/2017/PN.PTK) PATIK: Legal Journal, Volume 06 Number 03, December 2017.

Novinna, V. (2020). Consumer protection from Dissemination of Personal Data by Udayana Master of Law Journal, 9(1). Ramiyanto, (2017), Electronic Evidence as Valid Evidence in Law Criminal Procedure, Law Journal and Justice, Vol. 6, No. 3

Rani, M. (2014). Service Authority Protection Finance Against Confidentiality And Security of Customer Personal Data Bank. Straits Journal, 2(1).

Legislation

Law Number 11 of 2008 concerning Electronic Information and Transactions has been changed by law Number 19 of 2016 concerning Information and Electronic Transactions.

Criminal Code (KUHP).

Law Number 10 of 1998 concerning Banking, amendments to Law Number 7 of 1992.

Law Number 8 of 1999 concerning Consumer Protection.

Law Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions

Law Number 8 of 1999 concerning Consumer Protection.

Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector,

Jurnal

DAFTAR PUSTAKA 871/Pid.sus/2017/Pn.Ptk)PATIK: Jurnal Hukum, Volume 06 Nomor 03, Desember 2017.

Novinna, V. (2020). Perlindungan Konsumen

Astrini, D. A. (2015). Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime. Lex Privatum, 3(1), 149–160

Cynthia, H., 2018, "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia",Jurnal HAM, Vol.9, No.2.

Irwan Sugiarto, Hari Sutra Disemadi. (2020).

Consumers Spiritual Rights In Indonesia: A Legal Study Of Sharia Fintech Implementation In The Consumers Protection Perspective.

Jurnal Ius Kajian Hukumdan Keadilan,Vol 8,No 3. Jovin Ganda Ramdhan dan Sumiyati,

Perlindungan Hukum Terhadap Nasabah Korban Skimming Ditinjau Dari Undang Undang Nomor 8 Tahun 1999,Volume 12. No. 1 hal 89 Jurnal magister hukum , tanggung jawab kejahatan perbankan melalui modus operandi skimming Volume7|Nomor 1| Maret 2020 Hal 37 Lex Privatum Tentang Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime Vol.III/No.1/hal 149

Manulang, Sitohang. (2017).

Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Pemalsuan Dokumen Milik Orang Lain Untuk Pinjaman Online (Studi Putusan Nomor dari Penyebarluasan Data Pribadi oleh Pihak Ketiga: Kasus Fintech "Peer to Peer Lending".Jurnal Magister Hukum Udayana, 9(1).

Ramiyanto, (2017), Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana, Jurnal Hukum dan Peradilan, Vol. 6,No. 3

Rani, M. (2014). Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank. Jurnal Selat, 2(1).

Peraturan Perundang-Undangan

Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik.

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan perubahan atas Undang- Undang Nomor 7 Tahun 1992.

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Undang-Undang Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan,