

Protection of Bank Customers in Savings Account Hacking Through Illegal Links



Muhamad Shafwan Afif¹, Yansiska², Theresia Anita Christiani³

^{1,2}Students Of Magister Of Law Program, Universitas Atma Jaya Yogyakarta, Indonesia

³Lecture Of Faculty Of Law Program, Universitas Atma Jaya Yogyakarta, Indonesia

ABSTRACT: Research regarding the protection of bank customers in savings account hacking through illegal links aims to determine legal protection for bank customers who are victims of burglary of savings accounts via illegal links based on the Indonesian ius constitutum. Customers are important people in the banking world and the security of both their data and savings must be maintained, however, there are still many irresponsible individuals who steal bank customer data through any application. The results of this research are that there is no ius constitutum regarding burglary via illegal links, but currently what can be used as legal protection for bank customers who are victims of cases of burglary of savings accounts via illegal links is Article 52 paragraph (2) of Law Number 10 of 1998 concerning Banking, then Article 28 paragraph (1) of Law Number 11 of 2008 concerning Information and Electronic Transactions, Article 362 of Law Number 1 of 1946 concerning Regulations on Criminal Law (KUHP).

KEYWORDS: Law, Bank, Account Hacking, Illegal Links

the era of globalization, many changes have been made, especially changes in the technology field, which are marked by the shift in media from print media to digital media using the internet in the form of websites or applications that support it. The transaction system in Indonesia has been affected, namely by using systems based on internet technology so that what was originally an ordinary transaction has now changed to an electronic transaction. [1] These changes are also experienced by institutions or agencies operating in the financial sector, both private and public, for example, banks. Banks are categorized as institutions whose function is to be a place to store people's wealth in the form of money and have a responsibility to the people who store them known as customers to safeguard the customers' money. Not only money, but banks also have to protect the identity of their customers, unless certain conditions the bank is allowed to provide customer data such as for court purposes and so on as stated in Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking.

Customer data is very important and has its exclusivity because in principle this data is data that can only be owned by the financial institution and the customer. Customer data is very exclusive because it contains information that they own and must not be disseminated to outside parties or unauthorized parties. Indonesia has more than one regulation to guarantee the security of customer data, as is the case in Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, Bank Indonesia Regulations number 22/20/PBI/2020 concerning Bank Indonesia Consumer Protection, Financial Services Authority Regulation number 11/2022 concerning the Implementation of Information Technology by Commercial Banks, and finally in Financial Services Authority Circular Letter number 4/SEOJK.07/2014 concerning Confidentiality and Security Consumer Data or Personal Information.[2]

The fact that we often find in the field is that there are still efforts to fight ius constitutum carried out by irresponsible individuals in the form of leaking or taking data and taking money deposits from bank customers without the knowledge of the bank and the customer. Bank customer data leaks in Indonesia are currently still the center of attention for all components of society, especially in this digital era, all levels of society entrust their finances or funds stored in banks, this is based on the easy conditions for opening deposits, the use of bank deposit facilities is also very easy and can be accessed for 1 full day within 24 hours, even in the hand. The term in this hand refers to the cellphone mediator as a tool used to carry out banking transactions with features provided by the bank known as mobile banking. As time goes by, people rely on mobile banking for their banking transaction

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

needs without paying attention or considering the security of confidentiality of customer data, which is used by irresponsible individuals. Currently, media are reporting this, such as Jogjaaja.com, which reports that there are many modes of fraud through clicking links on the WhatsApp application in the name of government or private institutions. [3] Detik Jatim also wrote news about Irwan Gema who was a victim of fraud in the form of clicking on illegal links in the eastern Java region (JATIM) and lost Rp. 549 million rupiah. [4] CNN Indonesia on Thursday 20 July 2023 wrote news that the Director General of Applications and Information at the Ministry of Communication and Information, Samuel Abrijani Pangerapan, said that there had been 94 cases of information leaks in Indonesia starting around 2019, and 35 of them occurred in 2023.[5] The news portal Kompas.com also wrote a news article on May 16 2023 that several experts believed that BSI had been hit by a ransomware-type cyber attack.[6]

There have been many previous studies regarding the legal basis for victims of bank customer leaks, such as Fanany's (2020) research with the title "Legal Protection of Bank Customer Personal Data (Case Study at PT Bank Jatim, Mojokerto City Branch)" which focuses on the researcher's analysis of the legal basis. owned by a bank customer regarding personal data. The strength of this research lies in the perception it creates, especially regarding the existing guidelines in Indonesia regarding the legal basis for customer personal data and also the several ways in which the object of the research, namely PT Bank Jatim, Mojokerto City Branch, specifically protects its customers. [7] The weakness of this research is that it only uses 1 type of ius constitutum, namely Law number 10 of 1998 concerning Banking. So, in this research, there is a difference, namely using other ius constitutum such as Law number 27 of 2022 concerning the Protection of personal data.

Another research conducted by Tarantang (2023) with the title "Legal Protection of Bank Customers in Digital Transactions", in this scientific paper analyzes that legal protection of bank customer data is interrelated with the protection of human rights. This research has advantages, because it offers a new legal basis that to protect a customer, the 2008 Information and Electronic Transactions Law can be used.[8] The weakness of this scientific paper is that it does not provide information regarding the protection received by victims of bank account burglary. Based on this description, this research has novelty, especially in explaining the basis for legal protection by victims of bank savings accounts hacked via illegal links.

Meanwhile, research conducted by Sudjana (2022) entitled "Leaking Bank Secrets as a Violation of Privacy Rights and Electronic Personal Data of Bank Customers", in this research analyzes the responsibilities of banks and their regulations. The advantage of this research is that it explains the bank's responsibility for leaking customer personal data.[9] The weakness of this research is that it does not provide a definite explanation about the consitutum for victims of bank account hacking via illegal links. Based on this description, this research has an update, namely linking the theory of legal certainty with the importance of an ius consitutum regarding the burglary of savings accounts through illegal links.

Previous research only focused on the bank's point of view and also the legal basis that protects bank customers in carrying out their activities, but on the other hand, there is a lack of information or explanation regarding ius consitutum regarding victims of savings accounts being hacked through illegal links. Meanwhile, this research has updates, emphasizing the importance of regulations for victims of breaches in bank savings account data via illegal links which are linked to the theory of legal certainty. This research aims to determine protection for bank customers in cases of burglary of savings accounts through illegal links based on the ius constitutum in Indonesia. Based on the objectives of this research, the problem formulation is: How is protection for bank customers in cases of burglary of savings accounts through illegal links based on the ius constitutum in Indonesia?

I. METHODS

This legal research takes the form of normative juridical research by concentrating on cases viewed from the perspective of norms that are in harmony with current problems. Information collection uses library data collection techniques by utilizing information sources starting from the main important materials, namely Banking Law number 10 of 1998, Personal Data Protection Law number 27 of 2022, as well as the Criminal Code which has not yet been updated. Legal research supporting materials use theories, principles, and research results in books, scientific journals, and websites that discuss customer protection, personal data protection, and cybercrime from trusted sources.[10] The analytical method uses qualitative analysis by connecting cases with norms, principles, theories, or research results to give rise to a deductive conclusion in this research.[11]

II. RESULT AND DISCUSSION

A. Legal Certainty Theory

The idea regarding the principle of legal certainty was originally explained by Gustav Radbruch in a book entitled "*einführung in die rechtswissenschaften*" which states that there are 3 basic legal values, namely the first is justice, the second is benefit, and the last is legal certainty. A legal certainty is a form of guarantee of justice contained in the law, where we know that there is the adigium *Lex nemini operator iniquum, neminini facit injuriam* "the law does not give injustice to anyone and does not wrong

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

anyone". Another opinion was expressed by Lord Lloyd who said that if there is no legal certainty then uncertainty will arise and this uncertainty can result in fights.[12]

The theory of legal certainty was presented by Michael Jefferson, he argued that a law must have elements such as the law must not be vague, the legislative body is prohibited from creating laws that apply retroactively, the judiciary is prohibited from creating new offenses, and the criminal code must be interpreted strictly. According to Michael Jefferson's view, the law must be firm, there must not be multiple interpretations and the application of the law must remain firm by the principle of legality. Magnis-Suseno also believes that the principle of legal certainty is legality which is an important element in the concept of the rule of law.[13]

Legal certainty can be interpreted as a principle that applies in the world of law, which is useful for guaranteeing the strength of a legal product so that it does not cause uncertainty and also as a guideline for a good society. This is in line with the purpose of law put forward by Peter Mahmud Marzuki, he believes that everything in the universe has its purpose, including law. Law has the aim of being a guide for society regarding activities it carries out in the environment.[14]

B. Protection For Bank Customers In Banking Law Indonesia

If the law is grouped based on the period it comes into force, it is divided into 2 forms, namely *ius constitutum* and *ius constituendum*, the meaning of *ius constitutum* is law that has been in force and is being used by a particular government system, the popular term is positive law, while *ius constituendum* is a law that has not yet been implemented. ratified and stipulated by the competent government, so that it can be interpreted that the law is proclaimed, the popular term is a draft law or *prolegnas*. The function of *ius constitutum* is as a tool to regulate public order in social relations, so the law will always respond to changes and developments in people's behavior in its environment.[15] To maximize the function of law as a tool for regulating society, it goes through a series of processes that are quite numerous and must involve the role of citizens by the zone the law applies to obtain good quality legal products.[16] The series of processes can be started by observing social phenomena and changes in society, then the results are expressed in the form of norms in a draft law using legal language rules by the next big Indonesian dictionary reference called KBBI which contains orders and sanctions for violators, the final authorized by the government authorized by applicable law. *Ius constitutum* was created with the aim of the good of society, but it must be balanced with law enforcement that is running well because if law enforcement is not running well it can cause the articles in the law to be dormant and deemed to have failed to achieve their goals. [17] These things have fundamental similarities with legal theory relating to justice as put forward by several experts such as Gustav Radbruch who holds the view that the value of justice is "material" which must be the substance of legal standards, while valid rules are "structures" which must be maintaining the value of justice, then W.A.M. Luypen has another opinion that regulatory arrangements should be directed at equality. Justice is a fundamental standard in regulations because justice is contained in the content of a regulation which is obtained from interpreting a legal product.[18]

Indonesia, within the scope of wealth storage, has an institution, namely banking. Banking institutions have the aim of helping the implementation of community development to improve justice, monetary development, and community stability in seeking government assistance for the wider community, this is by the points in the fifth principle of Pancasila, namely social justice for all Indonesian people. The era of technological progress has made banking institutions innovate in the form of Internet Banking, which is a service for carrying out banking activities via the Internet network. *Internet Banking is a development that uses web innovation as a mode to complete exchanges and obtain data in the form of mobile banking or bank websites. This innovation uses the internet network as a means of connecting customers with the bank so that there is no need for face-to-face meetings on the spot.* [19] Customers can use a PC, tablet, PC, or cellphone connected to the internet network to connect customers with the bank system. E-banking is a technological innovation used by banks to fulfill the desires of customers who need financial services that are faster, more reliable, more concise, and affordable and can be accessed from anywhere. Regulations regarding Internet banking services are contained in Bank Indonesia Regulation number 9/15/PBI/2007 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks.[20]

The protection provided by the authorized government based on *ius constitutum* to bank customers is divided into 2 types, namely preventive and repressive.[21] Repressive legal protection takes the form of taking action and imposing sanctions such as administrative, criminal, prison, fines, and other additional penalties by the *ius constitutum*. This repressive effort is regulated in Article 52 paragraph (1) of Law number 10 of 1998 concerning Banking, which states that Bank Indonesia provides administrative sanctions to banks that commit acts of default or the leadership of Bank Indonesia has the option to refuse the dangerous bank's operating permit. Article 52 paragraph (2) of Law number 10 of 1998 concerning Banking regulates the types of administrative sanctions ranging from material fines to being branded as a dishonorable person in the banking world. In Article 100 paragraph

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

(1) of the Republic of Indonesia Government Regulation number 71 of 2019 concerning the Implementation of electronic systems and transactions, it is regulated that administrative sanctions may be imposed. [22]

Apart from repressive efforts, there are also preventive efforts that aim to protect customers from efforts that could harm them and from efforts to violate the law by irresponsible individuals. This preventive effort is regulated in article 1 point 28 of Law number 10 of 1998 concerning Banking which regulates bank secrecy as everything related to information, data about customers and their investment funds. In Article 40 paragraph (1) of Law number 10 of 1998 concerning Banking, it is also regulated that banks must keep information and data about customers and their savings funds confidential.[23] Other regulations that support the confidentiality of customer data are regulated in Article 44 paragraph (1) of Financial Services Authority Regulation number 11 of 2022 concerning the Implementation of Information Technology by Commercial Banks which regulates banks' obligations to realize the principle of protecting personal data when processing it, Article 45 paragraph (1) letter e also regulates that banks are obliged to establish personal data security to realize personal data protection when data exchange activities.[24] *Ius constitutum personal data protection is a manifestation of the 1945 Constitution of the Republic of Indonesia Article 28G paragraph (1) which regulates that every person has the right to protection of himself and his family, honor, dignity, and property under his control, as well as the right to a sense of security and protection from the threat of fear of doing or not doing something that is their human right.*[25] The problem of protecting individual information arises because of concerns that individual information could be misused by irresponsible individuals or groups unlawfully. This violation causes material and immaterial losses for the victim.

Legal protection for customers who provide personal data to banks is regulated in Article 10 paragraph (1) of Law number 27 of 2022 concerning the Protection of personal data which regulates that personal data subjects have the right to submit objections to decision-making actions that are based solely on processing. automated services, including profiling, that give rise to legal consequences or have a significant impact on the subject of personal data.[26] Article 10 paragraph (2) stipulates that further arrangements regarding objections to processing are automatically regulated in Government Regulations. If material and immaterial losses occur, the owner of personal data or the customer has the right to file a lawsuit and/or receive compensation by Article 12 paragraph (1) of Law number 27 of 2022 concerning the Protection of personal data which states that the individual subject of information has the privilege to sue and get rewards for violations of handling its information by legal guidelines".

C. Cybercrime Via Illegal Links

Cybercrime is a crime in the form of misuse of internet technology, it can be stated as an unlawful act committed intentionally using the internet system based on the sophistication of computer and telecommunications technology. The Encyclopaedia Britannica book discusses cybercrime, namely the use of computer devices to carry out illegal acts, for example, identity theft, fraud, trafficking in pornographic content, and violation of privacy. Cybercrime and conventional crime have striking differences in terms of the use and utilization of technology. Aep S. Hamidin categorizes cybercrime crimes according to their types, namely:

1. *Unapproved Access;*
2. *Unlawful Items;*
3. *Conscious spread of infection;*
4. *Information Fabrication;*
5. *Digital undercover work, harm, and coercion;*
6. *Cyberstalking;*
7. *Carding;*
8. *Hacking and saltine;*
9. *Cybersquatting and typosquatting;*
10. *Piracy;*
11. *Cyberterrorism.*[27]

Legal links are a combination of two syllables, namely link and illegal, links are also known as url. Prayogi thinks that a link is a unified series of characters created based on certain standards to indicate an address on an internet network, while Sora's opinion is that a link is a series of characters that are deliberately arranged based on certain formatting rules, then used to describe an internet address in the form of text. , images, and files on the internet network.[28] Illegal has the meaning in the next major Indonesian dictionary reference called KBBI that is not based on the law or against the law. An illegal link can be interpreted as an electronic internet address that is useful as a domain and can be detrimental to its users because it is illegal or against the law with impacts in the banking world in the form of forced access to customers' data and can drain customers' savings, thereby causing great harm to customers.

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

The way to use this illegal link which is intended for theft in the banking sector is by clicking or inputting a link whose truth and authenticity we do not know, then it is automatically synchronized with the customer's mobile banking. There are many types and modes of sending illegal links to targets, including:

1. Through an illegal link sent via the WhatsApp application;
2. Through illegal links sent via Google Drive;
3. Through an illegal link sent via the Instagram application;
4. Through illegal links sent via email;
5. Through illegal links sent via the Facebook application;
6. Through illegal links sent via the Twitter application;
7. Through illegal links sent via a pop-up window;
8. Via illegal links sent via short message (messenger).

The use of legal links for criminal acts is usually reserved for crimes based on fraud and theft. This is because the main concept of using illegal links aims to take the victim's data by force and without the victim's consent, then use this data irresponsibly. For banking institution customers who are affected by the use of this illegal link, it can result in the customer's savings being lost and all being drained/taken by fraudsters via illegal links.

The ius constitutum in Indonesia currently states clearly regarding illegal links. There are no regulations yet, but there are several IUS constitutums that have the same elements regarding fraud via illegal links and there are also laws that can be the basis for regulations for a bank customer to feel safe in carrying out savings deposit activities, these regulations include the Constitution of the Republic of Indonesia of 1945, Law number 10 of 1998 concerning Banking, Law number 11 of 2008 concerning Electronic Information and Transactions, Law number 1 of 1946 concerning the Criminal Code, Law number 27 of 2022 concerning Personal Data Protection, Government Regulation number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. Based on the ius constitutum that has been explained, it can more or less create a sense of security and comfort for bank customers in the form of savings accounts.

D. Analysis

The Directorate of Cyber Crime, Bareskrim Polri, revealed that when taking bank customers' savings, the perpetrators had their fields of work. The perpetrator's first stage was in the field of application creation (APK) and its development. Apart from that, there was also the role of the perpetrator team to collect a database of potential victims whom they had targeted with the consideration that the potential victims were passive savings customers. *Fraudsters then drain savings accounts through their applications and carry out forced balance withdrawals which are against the law.* [29] According to Teguh Aprianto, a security practitioner, Cybersecurity Consultant, and Founder of Ethical Hacker Indonesia, via his tweet on the X @secgron account, during 2023 customer data leaks will continue to increase and there is no solution or certainty that someone will maintain the confidentiality of their data. It is proven that up to September 2023, there were still many cases of customer data theft among state institutions. In early October 2023, it was reported that OJK was the victim of a Royal ransomware (Blacksuit) attack, which was confirmed by OJK and had an impact on OJK's internal and external services being paralyzed and there was no resolution yet. Teguh Aprianto has created a page www.periksadata.com to check whether our data has been leaked or not.

According to checkeddata.com records, so far as of September 26, 2023, more than 5 billion personal data has been leaked and there has been no definite response from the government. In its development, there is a cybercrime called Fraud Mode, changing customer data through illegal links, namely:

1. Fraudster contacting customers via WhatsApp by sending a link that is suspected to be illegal, accompanied by information in the opening sentence to get a package, gift, or wedding invitation;
2. The customer clicks on a link that is suspected to be illegal in APK format or other format which directs the customer to fill in an online form in the form of a telephone number and email;
3. From the results of inputting customer data on the allegedly illegal link, the customer gets an OTP (One Time Password) password, which is a secret code when making transactions or carrying out online activities which is sent to the customer's telephone number. The OTP password received by the customer is handed over unconsciously to the fraudster to change the customer's data;
4. The impact is that with customer data that has been changed, fraudsters can gain access to customers' mobile banking and/or request mobile banking activation;
5. Fraudster Fraudsters who succeed in accessing customers' mobile banking then carry out account debit transactions which result in material losses.

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

The act of fraud using illegal links is an activity of fraud and theft because this act contains an element of coercion for the personal gain of the perpetrators. If we use the interpretive analysis method that we associate with the existing *ius constitutum*, several articles can be charged that have elements similar to fraud via illegal links, although currently there has not been a phrase in the norms of legislation that uses the phrase illegal links until this writing was written.[30] Articles that can trap the perpetrator include Law number 11 of 2008 concerning Information and electronic transactions, Article 45 paragraph (2) which regulates that every person who has fulfilled the components as intended in Article 28 paragraph (1) will receive a maximum prison sanction of 6 years and/or a maximum fine of one billion rupiahs, meanwhile, Article 28 paragraph (1) regulates that every person who has no right and who deliberately conveys false and misleading news can cause losses to buyers on electronic exchanges. Still in the same *ius constitutum* Article 46 paragraphs (1) to paragraph (3) regulates that people who fulfill the components of Article 30 can be threatened with a maximum penalty of 8 years in prison and a maximum fine of Rp. 800,000,000,-, Article 52 paragraph (3) also regulates that any person who violates the provisions of Article 30 belonging to a central banking, banking, or financial institution will have the penalty added to two-thirds of the sentence, Article 30 which is the source of Article 46 and Article 52 regulates that every person who does not have the right to access a computer/ Electronic systems have a place with others. In the old version of the Criminal Code, cases of fraud via illegal links could be subject to Article 362 of the Criminal Code which stipulates that every person who commits an act of taking someone else's property against the law is threatened with an act of theft with a maximum prison sentence of 5 years or a maximum of 900 rupiah. , Article 378 of the Criminal Code can also ensnare perpetrators of illegal link fraud with elements of fraud and the threat of a maximum prison sentence of 4 years. Apart from that, Bank Indonesia can also impose administrative sanctions on banks that do not fulfill their obligations by the *ius constitutum* or the leadership of Bank Indonesia can revoke the business license of the bank concerned as regulated in Article 52 paragraph (2) of Law number 10 of 1998 concerning Banking. [31]

III. CONCLUSION

Based on the problem formulation, namely how to protect bank customers in the case of burglary of savings accounts through illegal links based on the *ius constitutum* in Indonesia, the conclusion is that currently, cyber crime via illegal links is rampant in Indonesia, but for protection there is still no special *ius constitutum* regarding legal protection for victims of illegal link fraud crimes, especially bank customers. The principle in legal science is to recognize the term *Lex Specialis Derogat Lex Generalis* which can be interpreted as special rules overriding general rules and for illegal link fraud it is necessary to make special rules, but for now, *ius constitutum* can be used as legal protection for bank customers who are victims of burglary cases. savings accounts via illegal links are contained in Article 52 paragraph (2) of Law Number 10 of 1998 concerning Banking, then Article 28 paragraph (1) of Law Number 11 of 2008 concerning Information and Electronic Transactions, and Article 362 of Law Number 1 of 1946 concerning Regulations on Criminal Law (KUHP). Currently, there are no regulations governing the compensation that can be received by bank savings customers who suffer losses and the efforts that can be made by victims of hacking through illegal links, so the only effort that victims can make is to report it to the authorities. A customer is someone who entrusts their savings to a financial institution, namely a bank, but currently, there is no positive law to provide a sense of security to these customers, so victims of cybercrime in the form of illegal links are still not guaranteed security, which results in losing their savings balance.

ACKNOWLEDGMENT

Gratitude to the founders and Co-Founders of the Law Faculty of Universitas Atma Jaya Yogyakarta and also thank you to Mrs. Theresia Anita Christiani and Mrs. Sundari who have guided the process of writing this scientific work.

REFERENCES

- 1) Choirul Anam, "E-Money (Uang Elektronik) Dalam Perspektif Hukum Syari'ah", *Jurnal Qawanin* 2, no.1 (2018): 95-112.
- 2) Republik Indonesia, "Surat Edaran Otoritas Jasa Keuangan (SE-OJK) Nomor 4 tahun 2014 Tentang Kerahasiaan Dan Keamanan Data Dan/atau Informasi Pribadi Konsumen.
- 3) Jogja aja, "Begini Ragam Penipuan Nasabah Bank Via Klik Link di WA dan Cara Menghindarinya", <https://jogjaaja.com/read/begini-ragam-penipuan-nasabah-bank-via-klik-link-di-wa-dan-cara-menghindarinya>, 26 September 2023, jam 21.38 WIB.
- 4) Denza Perdana, "Modus Bahaya Link WhatsApp Bobol Rekening Nasabah hingga Miliaran Rupiah", <https://www.detik.com/jatim/hukum-dan-kriminal/d-6823700/modus-bahaya-link-whatsapp-bobol-rekening-nasabah-hingga-miliaran-rupiah>, 26 September 2023, jam 22.00 WIB.

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

- 5) CNN, "4 Kasus Kebocoran Data Semester I 2023, Mayoritas Dibantah", <https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah>, 18 September 2023, jam 23.30 WIB.
- 6) Galuh Putri Riyanto, "Data Nasabah BSI Diduga Disebar Hacker, Kominfo Bicara Soal Ancaman Sanksi", <https://tekno.kompas.com/read/2023/05/16/11340077/data-nasabah-bsi-diduga-disebar-hacker-kominfo-bicara-soal-ancaman-sanksi>, 19 September 2023, jam 13.30 WIB.
- 7) Nadiyah Octavia Fanany, "Perlindungan Hukum Terhadap Data Pribadi Nasabah Bank (Studi Kasus di PT Bank Jatim Cabang Kota Mojokerto)", *Dinamika, Jurnal Ilmiah Ilmu Hukum* 26, no. 2 (2020): 136-146.
- 8) Jefry Tarantang, Ibnu Elmi A.S. Pelu, Wahyu Akbar, Rahmad Kurniawan, dan Aldina Sri Wahyuni, "Perlindungan Hukum Terhadap Nasabah Bank Dalam Transaksi Digital", *Morality : Jurnal Ilmu Hukum* 9, no. 1 (2023): 15-25.
- 9) Sudjana, "Pembocoran Rahasia Bank Sebagai Pelanggaran Hak Privasi dan Data Pribadi Elektronik Nasabah Bank", *Refleksi Hukum* 6, no. 2 (2022): 247-266.
- 10) Dr. Jonaedi Efendi, & Prof. Dr. Johnnya Ibrahim, *Metode Penelitian Hukum Normatif Dan Empiris* (Depok: Prenadamedia Group, 2018). Hlm 123.
- 11) Heri Retnawati, *Analisis Kuantitatif Instrumen Penelitian (Panduan Peneliti, Mahasiswa, dan Psikometrian)* (Yogyakarta: Parama Publishing, 2016), Hlm 41.
- 12) Mario Julyano dan Aditya Yuli Sulistyawan, "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum", *Jurnal Crepido* 1, no. 1 (2019): 13-22.
- 13) E. Fernando M. Manullang, *Legisme, Legalitas dan Kepastian Hukum* (Jakarta: Kencana, 2017), Hlm 159.
- 14) Oemar Moechthar, *Eksistensi, Fungsi, Dan Tujuan Hukum Dalam Pespektif Teori dan Filsafat Hukum* (Jakarta: Kencana, 2020), Hlm 87.
- 15) Muhamad Shafwan Afif, dan Heru Sugiyono, "Perlindungan Hukum Bagi Pemegang Merek Terkenal Di Indonesia", *Jurnal USM Law Review* 4, no. 2 (2021): 565- 585.
- 16) Dr. Budi Pramono, *Sosiologi Hukum* (Surabaya: Scopindo Media Pustaka, 2020), Hlm 26.
- 17) Nailah Artanti, Annisa Nurbaiti, dan Wahdan Arum Inaati, "Pengaruh Tekanan Eksternal, Ketidakefektifan Pemantauan, Opini Auditm Dan Pergantian Direksi Terhadap Kecurangan Laporan Keuangan (Studi Pada Perusahaan Keuangan Sub Sektor Perbankan Periode 2016-2020) ", *E-Proceeding of management* 10, no. 2 (2023): 1476-1484.
- 18) Prof. Dr. Peter Mahmud Marzuki, *Teori Hukum* (Jakarta: Kencana, 2020), Hlm 30.
- 19) Salsabila Putrianda, "Analisis Hukum Terhadap Perlindungan Nasabah Dalam Menggunakan Internet Banking Di Indonesia (Studi Kasus Bank X)", *Dharmasiswa* 2, no. 3 (2022): 1469-1478.
- 20) Republik Indonesia, "Peraturan Bank Indonesia Nomor 9 Tahun 2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi informasi Oleh Bank umum.
- 21) Apriani Rani, Grasia Kurniawati, Devi Siti, dan Hamzah Marpaung, "Perlindungan Hukum Nasabah Bank Dalam Hal Terjadinya Kesalahan Sistem Yang Mengakibatkan Perubahan Saldo Nasabah", *Syiar Hukum Jurnal Ilmu Hukum* 18, no. 2 (2020): 135-150.
- 22) Republik Indonesia, "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik", Pasal 100 ayat (1).
- 23) Republik Indonesia, "Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan", Pasal 40 ayat (1).
- 24) Republik Indonesia, "Peraturan Otoritas Jasa Keuangan Nomor 11 Tahun 2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum", Pasal 44 ayat (1).
- 25) Republik Indonesia, "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945", Pasal 28 G ayat (1).
- 26) Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi", Pasal 10 ayat (1).
- 27) Akbar Galih Hariyono, dan Frans Simangunsong, "Perlindungan Hukum Korban Pencurian Data Pribadi (*Phising Cybercrime*) Dalam Perspektif Kriminologi, *Bureaucracy Journal:Indonesia Journal of Law and Social-Political Governance* 3, no 1 (2023): 428-439.
- 28) Ahmad Martani, Saripuddin M, dan Nurul Ikhsan, "Design and Build a Company Profile Website Based on the Bootstrap Framework and Code Igniter Framework At The Foundation Independent Scholar Caliph", *Jurnal Multidisiplin Madani* 2, no.6 (2022): 2895-2912.
- 29) Farih Maulana Sidik, " Bareskrim Ungkap Peran 13 Penipu Modus Kirim APK-Link yang Kurang 493 Rekening", <https://news.detik.com/berita/d-6524267/bareskrim-ungkap-peran-13-penipu-modus-kirim-apk-link-yang-kuras-493-rekening>, 11 Oktober 2023, 20.45 WIB.

Protection of Bank Customers in Savings Account Hacking Through Illegal Links

- 30) Anton Hendrik Samudra, "Modus Operandi Dan Problematika Penanggulangan Tindak Pidana Penipuan Daring", *Mimbar Hukum* 31, no.1 (2019): 59-74.
- 31) MOHD.Yusuf Dm, Addermi, dan Jasmine Lim, "Kejahatan *Phising* dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia", *Jurnal Pendidikan* 4, no.5 (2022): 8018-8023.



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.