GLOBAL INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

https://global-us.mellbaou.com/

Open Access

Cite this article: I Putu Budi Astika et al. (2024). Legal Protection Of Fund Saving Customers Against Cyber Phising Acts In Indonesia. Global International Journal of Innovative Research, 2(8). https://doi.org/10.59613/global.v2i8.285

Received: July, 2024
Accepted: August, 2024

Keywords:
Bank, Cybercrime , Phishing , Protection law

Author for correspondence:
I Putu Budi Astika
E-mail: budiastka44@gmail.com

Published by:

GLOBAL SOCIETY PUBLISHING

Legal Protection Of Fund Saving Customers Against Cyber Phising Acts In Indonesia

[1]I Putu Budi Astika, [2]I Nyoman Sujana, [3]I Ketut Arya Wijaya Caste

[1,2,3]Universitas Warmadewa, Denpasar, Bali, Indonesia

Study thesis This analyze about Legal Protection for Customers Saving Funds Against Cyber Phishing in Indonesia. As for focus study This is regarding (1) how cyber phishing phenomenon in scope banking in Indonesia? and (2) how protection law to customers internal fund storage cyber phishing acts in Indonesia? Study This use approach normative ones with choose type study the aim For research governing rules /norms How protection law customers saving funds against cyber phishing acts in Indonesia. Writer study with theory certainty law and theory protection law , which with second knife analysis the writer produce Conclusion (1) The phenomenon of cybercrime with form phishing later This the more massive happened in Indonesia with so rapidly development technology in Indonesia, OJK owns it authority supervise in sector finance until moment This Not yet publish or validate Special OJK regulations arrange matter that's what happened the absence of norms on crime cyber crime with form phishing in Indonesia and (2) Form protection law to customers depositors who become victims of cyber phishing preventive stated in OJK Regulation Number 22 of 2023 changes on OJK Regulation Number 6 of 2022 concerning Protection Consumers and Society in the Financial Sector in Chapter II of the Law as stated in Article 3 paragraphs (1), (2) and paragraph (3) and Article 20. Meanwhile form protection law repressive regulated in Bank Indonesia Regulation Number : 16/1/PBI/2014 concerning Protection System Services Consumers Payment in article 16 paragraphs (1) and (2) later also regulated in law Number 19 of 2016 changes on Constitution Number 11 of 2008 concerning Information and Transactions Electronics in Article 28 paragraph (1) and Article 45 paragraph (1).

1. Introduction

Economic development is a critical aspect of national growth, involving both government and private sector participation. In Indonesia, the banking sector has seen rapid growth over the past 25 years, playing a significant role in supporting economic activities by collecting public funds and providing credit. The Indonesian legal framework, guided by the 1945 Constitution and specific banking laws, ensures the stability and regulation of the banking sector.

Banks function as financial intermediaries, facilitating the transfer of funds between savers and borrowers, thereby supporting economic activities such as production, consumption, trade, and investment. The legal system in society plays a crucial role in shaping economic activities, emphasizing the interdependence of law and economics.

With technological advancements, traditional banking methods are evolving towards digital banking, enhancing efficiency and customer service. However, this shift has also led to new challenges, such as cyber phishing. This is exemplified by a recent case in Bali, where a local official lost a significant amount of money due to phishing. The study aims to explore the phenomenon of cyber phishing in Indonesia's banking sector and analyze the legal protections available to customers against such threats.

2. Method

Type of research used is study law normative , with approach Legislation (statute approach), approach case (case approach), approach historical (historical approach), approach conceptual (conceptual approach). Source material laws used and studied in research law normative classified become three type namely 1) materials primary law , 2) material law secondary , and 3) materials law tertiary . Analysis in study This use descriptive data analysis qualitative.

3. Result and Discussion

1. Phenomenon cyber phishing in scope banking in Indonesia

Legal Basis for Cyber Crime in the ITE Law

Cybercrime first emerged in the United States in the 1960s, with notable cases in the 1970s involving data manipulation, misuse of company computers, data theft for drug smuggling, and credit card fraud. In Indonesia, cybercrime became a serious concern as the country entered the era of globalization, with increasing influence from the cyber world on various aspects of life.

In response, Indonesia ratified Law No. 11 of 2008, later updated with Law No. 19 of 2016, concerning Information and Electronic Transactions (ITE). The ITE Law covers a range of issues: the first part addresses marketplace regulation, domain names, and electronic signatures; the second part deals with cybercrimes, including illegal content (such as hate speech, hoaxes, online fraud, and pornography) and illegal activities like hacking, interception, and data interference, as detailed in Articles 27-35.

Types of Crime Cyber

Crime with cyber media in other terms are called as follow criminal mayantara , internet crime, or internet crime originates from which the word cyber is taken from the word cybernetic which means One field science which is combination between robotics, mathematics, electricity, and psychology developed by Nortbert Wiener in 1948. One of application of cybernetics is field (robotic) control of distance Far . In terms of This of course that is desirable is A real control perfect (Harris Hardianto , 2019:31).
According to Sutanto, take action criminal cyber divided into two types , as following :

In the realm of cybercrime, technology, particularly information technology (IT), can play two distinct roles: as a facilitator of crime or as the target of criminal activities.

The first type of cybercrime involves the use of technology as a tool to commit various illegal activities. Examples of these crimes include piracy, which involves the unauthorized copying or use of intellectual property; fraud conducted through email; bank account fraud and theft; online gambling; terrorism; and the creation or dissemination of websites that promote harmful ideologies or hate speech related to ethnicity, race, or religion. Other examples include the illegal distribution of drugs and the facilitation of sex trafficking through online platforms.

The second type of cybercrime targets IT systems and infrastructure themselves. In these cases, criminals do not use computers and the internet merely as tools but rather as the objects of their criminal activities. This includes illegal access to computer systems, known as hacking; damaging websites or data servers, often referred to as cracking; and defacing websites to alter their content maliciously.

These two broad categories highlight the diverse ways in which cybercrime can manifest, with technology playing a central role either as a means or as a target in criminal activities.

Related crimes tightly with use computer and network based technology telecommunication in a number of literature and practice grouped in a number of form , including :

1. Unauthorized access to computer systems and services.
2. Illegal contents .
3. Data Forgery.
4. Cyber espionade .
5. Cyber sabotage and extortion.
6. Offense against intellectuals.
7. Infringements of privacy. (Maskun , 2013:54).

Cyber Crime Actions In The Scope Of Banking

Banking crime refers to illegal activities that violate laws governing the financial sector, involving offenses such as fraud, money laundering, corruption, and financial market manipulation. These crimes often harm financial institutions, customers, and society at large. Banking crimes are closely related to the banking industry and can involve institutions, systems, and banking products. Both banking insiders and customers can be involved, with perpetrators often exploiting system loopholes to evade detection. Customers can also fall victim to banking crimes through practices like phishing and skimming, where their financial data is stolen for fraudulent purposes.

Act crime cyber (cybercrime) in the sector service finance and banking in a way general divided into two (two) types namely :

1. Social engineering, is manipulation psychology somebody with objective For get information certain with method cheat in a way smooth , fine realized or No through telephone or speak direct .
2. Skimming, that is action theft information with method copy information contained on a magnetic stripe debit card or credit illegally . The skimming method is method used For steal information customer at the time transaction using an ATM. In running action crime This There are 3 (three) tools main used namely : skimmer, hidden camera, and keypad. The skimmer is working For record activity customers in use ATM machines , tools This capable recording the electromagnetic strip that was on the victim's card at the time card entered to ATM machine . Hidden cameras and keypads are used For record victim's activities at the time do inputting the PIN on the ATM machine (Cristian Henry Ratugangi , 2021:183).

As for technique base obtain information with various social engineering modes , there are 3 (three) which are the most common namely :

1. Phishing , technique phishing used by perpetrators with trick or manipulate the owners bank account so they provide data and information that can used For access account banking owned by customers . Fraud committed For get information confidential like a password with disguised as a person or business trustworthy in A communication electronics . Channels used as email, service message short (SMS), or spreading fake links on the internet for directs victims to websites that have designed For cheat .

2. Vishing, that is effort cheat do approach towards the victim for get information or influence the victim to do action . Usually communication done through telephone .

3. Impersonation, that is effort fraudster pretend to be someone else with objective For get information confidential.

The social engineering method is often used done fraudster including :

1. Internet banking fraud and online transactions using card credit / debit card , ie perpetrator confess as bank employee who informed exists change cost SMS/internet banking services , giving credit bonuses , distribution present invitations , etc. The perpetrator did it too fraud offer online loans with flower cheap .

2. Bank contact center, namely fraudster manipulate ATM machine so that the victim fails transactions and cards swallowed in the machine . When simultaneously , members team fraudsters standby around ATMs for direct the victim to contact call center number false . Tin pretends to be a call center false notify that the ATM has blocked , then ask the victim to give identity personal including ATM PIN number . The perpetrator is there around the victim then take The victim 's ATM card was swallowed in the machine .

3. Fraud SMS fraud , victims receive SMS content containing lure gifts , discounts , credit bonuses , tour packages , online loans and others . With pretext melt gift , the victim will provoked to ATM machine and directed For follow instructions given perpetrator like make fund transfers or top-up e-commerce balances.

Phenomenon Cyber Phishing In Indonesia

Digital banking, a product of financial technology, combines online and mobile banking into a single feature, allowing users to conduct transactions via their mobile devices. Unlike conventional banking, digital banks offer convenient access to services from anywhere, enhancing transaction ease. The Financial Services Authority (OJK) regulates digital banking through OJK Regulation No. 12/POJK.03/2018, which defines digital banking as services

developed electronically to optimize customer data use for faster, more convenient service. This regulation emphasizes the importance of technology, risk management, and infrastructure to support secure and reliable digital banking services.

The digitalization of banking has led to negative impacts, making it easier for criminal activities like identity theft, pornography, gambling, account hacking, and cyberattacks to occur. While e-banking offers advantages for both customers and banks, it also introduces risks, particularly regarding the theft of personal data. This information can be misused by unauthorized parties. The importance of protecting customer confidentiality is highlighted in Article 40 of the Indonesian Banking Law (amended by Constitution No. 10 of 1998), which mandates the protection of customer data beyond just financial information.

In 2023 BCA customers in Salatiga report lost balance IDR 68.5 million from the account through QRIS transactions . Then , BPD Bali customers lost Rp. 21.59 Billion Because conjecture burglary or hacking transaction illegal . Temporary That , the case that dragged BPD Bali occurred in April 2023 and was reported on May 15 2023. Head of Public Relations of the Bali Police, Commissioner Jansen Panjaitan , said report temporary enter in conjecture follow criminal hacking . However He confirm that case This Still in the investigation process.

It's rampant crime in form phishing the create form worries in the middle society in Indonesia. Lots of it people who are victims of deep cyber crime scope banking that's what causes it Very big loss , temporary That Not yet There is rule specifically regulated about crimes in the cyber world specifically in scope banking . In essence law must be give certainty use give justice in every hopeful individual law always present in various type lurking evil public.

2. Protection law customers deposit of funds against action cyber phishing in Indonesia Principles of Implementation in the Field Banking

About principle banking adopted in Indonesia can We know from provisions of Article 2 of the Law Number 10 of 1998 amendment on Constitution Number 7 of 1992 concerning Banking brought it up that , " Indonesian banking in do his business based democracy economy with use principle caution ". In carrying out connection partnership between the bank and its customers , to creation system healthy banking , activities banking need based with a number of principle . Before discuss about principles in banking , then important perhaps outlined about definition principle in room scope law . Principles according to SF. Marbun can means basis , cornerstone , fundamental principles , and soul or ideals . Principles can also be done understood as understandings and values that become point reject think about something (Lukman Santoso AZ, 2011:33).

For creating a healthy banking system in Indonesia following will outlined principle law banking in a way more detailed . that principle among others:

a. Principles of Economic Democracy .
b. Principle of Trust (Fiduciary Principle).
c. Principle of Confidentiality (Confidential Principle).
d. Precautionary Principle (Prudential Principle).

Principles in business banking is guidelines or values ethics that guide bank actions and policies operate activity his business . Principles This reflects expected high norms from financial institutions and are often fiat philosophical , ethical , and operational.

Legal Relationship Between Banks and Customer Creditors

Banks and customers are legal subjects, holding rights and obligations under the law. Legal subjects include humans and legal entities, with banks being a legal entity. The legal relationship between a bank and its customers is established through a binding agreement, as outlined in Article 1320 of the Civil Code, which requires mutual consent, legal capacity, a lawful object, and a legal cause. This relationship also involves the bank's obligation to maintain confidentiality regarding customer information. Customers who deposit funds into a bank enter into a legal relationship where the bank acts as the borrower of those funds. This relationship is governed by banking products like Current Accounts, Deposits, and Savings, where the bank is expected to manage these funds responsibly to generate profit.

Applicable provision in practice banking that customers who will depositing funds in a bank is carried out No with 'Free'. Customer entitled For accept flower on funds deposited with the bank . How big is this bro ? Look at the provisions that apply to each bank according to product existing banking . Customers also have right in a way specific , namely :

a) Customer entitled For know in a way detailed about products banking offered . This right is right main from customers , because without detailed explanation from the bank through its customer service , then it is very difficult customers For choose product banking what is appropriate with his will . Rights appa just will accepted by customers if customers Want to deliver the funds to the bank for managed .
b) Customer entitled For get flower deposit on product savings and deposits that have been made agreed moreover formerly . Customer entitled For :

1) Get service services provided by banks, such as facility ATM card .
2) Get report on transactions carried out through the bank.
3) Sue the bank in matter happen leak confidential customers .
4) Getland collateral come back , biila borrowed credit Already paid off .

5) Get auction money services in matter collateral for sale For pay off credit is not paid (April Atji Papendang , 2016:78).

Legal Relationship Between Banks and Customer Debtor

Article 1 number 11 of the Law Banking state credit is provision of money or bill that can be equalized with that , based on agreement or agreement loans between the bank and the other party obliges party borrower For pay off the debt after term time certain with giving flower . The elements contained in giving a facility credit is as following :

1. Trust

   Namely suati confidence giver credit provided (in the form of money , goods or services) will truly return at a certain time in the future . Trust This provided by the bank, where previously Already done study investigation about customers Good in a way internet nor external . Researchers and investigations about past and present conditions to customers applicant credit .

2. Agreement

   Beside element confidence within credits also contain element agreement between si giver credit with si recipient credit . Agreement This poured in a agreement where each party sign their respective rights and obligations .

3. Time period

   Every credit given own term time certain , term time This includes a return period credit that has been agreed . Term time the Can shaped term short , term intermediate or term long .

4. Risk

   There is something grace time return will cause a risk No uncollectible / jammed giving credit . The more long a credit the more big the risk and vice versa . Risk This become Bank liability , OK deliberate risks by negligent customers , as well as risks that are not on purpose . For example happen disaster natural or bankrupt business customers without element deliberate other .

5. Remuneration

   Represents profit on giving a credit or service that's what we are know with Name flower remuneration in form interest and fees administration credit This is bank profits . Whereas for banks based on Sharia principles reply his services determined with for results (Kasmir, 2017:88).

By general types credit can seen from various facet like credit normal investment used For needs business or build project / factory new or For needs rehabilitation . Example from credit investment for example For build factory or buy machines , there are also types working

capital credit used For needs increase production in operational . As example working capital credit given For buy material default , pay wages employee , or costs other related things with the Company's production process (Dadang, 2016:79).

Legal Protection for Customers Saving Funds Against Cyber Phishing In Indonesia

Electronic banking services allow customers to access information, communicate, and conduct transactions through electronic media. These services, which include online and mobile banking, use customer data to offer faster, more convenient, and secure banking experiences. According to Article 1 of POJK No. 12/POJK.3/2018, digital banking services are developed to enhance customer experience and are managed by dedicated units or functions within banks.

Banks use various delivery channels for electronic banking, such as ATMs, CDMs, phone banking, SMS, EDCs, POS systems, internet banking, and mobile banking. Electronic banking services include transactions like fund transfers, payments, and purchases.

Legal protection for customers includes preventive measures, like avoiding the transmission of sensitive information via insecure channels and being cautious with phishing attempts, and repressive measures to resolve disputes. The Financial Services Authority (OJK) mandates that financial service providers educate consumers about their rights and obligations, as outlined in POJK No. 1/POJK.07/2013 and OJK Regulation No. 22 of 2023. This includes implementing consumer protection principles in financial activities.

Paragraph (2) " Protection Consumers in the sector service finance apply principle :

a. Adequate education ;
b. Openness and transparency information products and/ or service ;
c. Fair treatment and behavior responsible business answer ;
d. Protection assets , privacy , and consumer data ;
e. Handling complaints and resolution effective and efficient disputes ;
f. Enforcement compliance ; And
g. Healthy competition . "

Protection law to bank customers in cyber phishing actions in form repressive experienced bank customers loss as a result of this action in accordance with Bank Indonesia Regulation Number : 16/1/PBI/2014 concerning Protection System Services Consumers Payment in article 16 paragraph (1) states that maintenance must own and implement mechanism handling complaint for consumer . Next , in paragraph (2) is mentioned that mechanism handler complaint as referred to in paragraph (1) is mandatory poured in form written

includes : a. Reception complaints ; b. Handling and resolution complaints ; c. Monitoring handling and resolution complaint .

Authorized agency in organize , supervise nor inspect in sector finance in Indonesia , namely OJK to moment This Not yet publish nor ratify special OJK regulations about cyber crime in scope banking in Indonesia. However , in 2008 the DPR of the Republic of Indonesia jointly with President The Republic of Indonesia ratifies Shrimp Act Republic of Indonesia Number 11 of 2008 then changed become Constitution Republic of Indonesia Number 19 of 2016 concerning Information and Transactions Electronics are next called with the ITE Law. Constitution the own objective For do arrangement and management information and transactions electronics at the National Level so that Technology Development Information can done optimally , evenly and spread to all over layer public use enlighten life nation and become tool important in activity life growth economy a more prosperous and just nation .

Articles that can ensnare doer and giver protection law customers deposit funds against cyber phishing actions in the ITE Law , namely in Article 28 paragraph (1) which states that " Every people with intentionally and without right spread news lies and misleading which resulted loss consumer in Transaction Electronics ". In CHAPTER XI regarding Provision Criminal Article 45A paragraph (1) of the ITE Law states " Everyone who is with intentionally and without right spread news lies and misleading which resulted loss consumer in Transaction Electronic as arranged in Article 28 paragraph (1) is punished with criminal imprisonment for a maximum of 6 (six) years and/ or finepaling a lot of Rp. 1,000,000,000,- (One Billion Rupiah).

4. Conclusion

The phenomenon of cybercrime, particularly phishing, has become increasingly prevalent in Indonesia due to rapid technological advancements. Despite the Financial Services Authority's (OJK) role in overseeing the financial sector, specific regulations addressing phishing and related cybercrimes have not yet been introduced, indicating a regulatory gap.

To protect victims of cyber phishing, legal protections are provided through both preventive and repressive measures. Preventive measures are outlined in the OJK Regulation No. 22 of 2023, which amends previous regulations to enhance consumer protection in the financial sector. Repressive measures include requirements set by Bank Indonesia Regulation No. 16/1/PBI/2014 for complaint handling, and provisions in the ITE Law (Law No. 19/2016)

that criminalize the dissemination of false information causing consumer harm. These legal frameworks aim to safeguard consumers and address the challenges posed by cybercrime.

5. References

Chatamarrasjid Ais, 2020, Indonesian National Banking Law , Kencana , Jakarta

Dadang Husen Sobana, 2016, Banking Law in Indonesia, CV Pustaka Setia, Bandung

Franky Ariyadi , 2024, Crime Secret Banking , Modus Operandi, and Cases Latest , CV. Nusantara Abadi Literacy , Malang

Haris Hardinanto , 2019, ILLEGAL ACCESS IN CRIMINAL LAW PERSPECTIVE, Setara Press, Malang

Johannes Ibrahim Kosasih, 2019, Access to Credit and Various Facilities Credit In Agreement Bank Credit , Sinar Gradika , East Jakarta

Johannes Ibrahim Kosasih, Hasan Haykal, 2020, Banks and Leasing Financial Institutions Strategic in Practice Business in Indonesia, CV. Mandar Maju, Bandung

Kasmir, 2017, Banks and Lemaba Finance Others , PT Rajagrafindo Persada , Depok

Lukman Santoso AZ, 2011, Legal Rights and Obligations of Bank Customers , Pustaka Yustisia , Yogyakarta

Maskun , 2013, Cyber Crime , cyber crime , Kencana Prenada Media Group, Jakarta

Rudyanti Dorotea Tobing , 2019, Banking Law Definition , Principles and Regulations , LaksBang PRESSindo , Yogyakarta

Zulfi Diane Zaini, Syopian Febriansyah , 2014, Legal Aspects and Functions of Guarantee Institutions Simpanan , Keni Media, Bandung

Annisa Indah Mutiasari , 2020, Development Industry Banking in the Digital Era , Vol. IX, No. 2

Aprilya Altji Papendang , 2016, Rights and Obligations Bank Customers and Legal Protection According to Constitution Number 10 of 1998, Vol 4, No. 3

Christian Henry Ratugangi , Anna S. Wahongan , Franky R. Mewengkang , 2021, Action Cyber Crime Crime in Activities Banking , Vol. 4, no. 5

Nani Widya Sari, 2018, Cyber Crime in Development Technology Information Based Computer , Vol. 5, no. 2.