Vol. 19 No. 4 March 2024

YURISDIKSI

Jurnal Wacana Hukum dan Sains

Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

Juridical Review of Cyber Security Mobile Banking Digitalization Process For Legal Protection of Customers

Florentina Dani Eti Kusuma Eko Wardani[1*], R. Febriarto Fadjar[1], Mychelvia Vrelya Giovanni Latuhihin[1]

[1] Faculty of Law, Pelita Harapan University, Indonesia

*Corresponding Author E-mail: email: florentina.dani@gmail.com

Article History: Received: December 16, 2023; Accepted: February 10, 2024

ABSTRACT

Indeed, the emergence of the bank's digitalization process does not necessarily eliminate the possibility of errors in its operation., both intentional and unintentional errors, one of the intentional errors is Fraud and/or cybercrime (as a crime that occurs through or on computer networks on the internet) in electronic services from this digitalization, which causes losses to other parties in the case of Digital Banks is the customer. Therefore, the purpose of this paper is to analyze the Security System of Digital Banking Services and Responsibility for Electronic Transactions of Digital Banking Services. In analyzing, the juridical-normative research method is used. The results showed that the realization of legal protection against customers for fraud or cybercrime that occurs in Digital Bank transaction activities can be seen from how the efforts of the government and the Authority in the Financial Services sector regulate and limit various interests and powers so that they do not collide with each other and are optimally organized. Commercial Banks are required to carry out their business activities prudently and implement Good Corporate Governance, Risk Management, and Consumer Protection will be better prepared to face various kinds of risks arising from the provision of Mobile Banking services, because if this is not done, the loss will be felt not only by service users but the Commercial Bank itself as a service provider, as can be seen in the case example in the decision.

Keywords: Cyber Security, Bank Digitization, Mobile Banking Customer Protection

1. INTRODUCTION

Basically, a bank is a business entity whose function is to collect and distribute public funds in the form of credit and/or other forms in order to improve the standard of living of the wider community. (Fure, 2016) As a financial services institution, banks manage their business by collecting funds from the public (*funding*), then distribute the funds to communities in need (*financing*/*lending*) and facilitate customers by providing effective and efficient payment mechanisms and tools (*banking services*). With this, banks can be useful as a source of increasing the flow of funds for productive investment.

As time goes by, competition is increasingly emerging in the Indonesian banking industry. Globalization indirectly forces the banking sector to follow the flow of changes in information technology and telecommunications. This phenomenon certainly stimulates banks in Indonesia to develop the quality of products and services they wish to distribute to their customers by utilizing information technology knowledge. Digitalization is not an option for banks, but rather an urgent matter that must be pursued and implemented.

ISSN print 2086-6852 and ISSN Online 2598-5892

Banking efforts to improve information technology through services to customers indirectly direct banks to a new era, namely the era of digital banking. (Paulus, 2019) The real manifestation of digital banking services (*digital banking*) can now be seen starting from opening an account, closing an account, to electronic-based financial transactions. Innovation and service provision as well as various strategies that emerge as a result of the use of information technology are not only aimed at standing tall against high competition, but also aim to make transactions easier for bank customers. Customers can easily access various banking services and products just via their mobile phone.

In supporting non-cash transactions, Bank Indonesia has also made moves to form provisions regarding payment system regulation, namely by issuing Bank Indonesia Regulation No. 22/23/PBI/2020 concerning Payment Systems ("Payment System PBI") which came into effect on July 1 2021. This PBI was prepared with the hope that it will produce effective and responsive payment system provisions including all aspects of payment system implementation in order to prioritize economic development and digital finance. (Emanuella, 2021)

The developments occurring in the banking sector are not without regulations that support the successful implementation of digital banking services. Law plays an important role in continuing to maintain harmony in a country, especially in important sectors which are pillars of the country's growth. Therefore, it is appropriate for law to develop along with advances in technology and information science. Financial Services Authority Regulation Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks ("POJK No. 12/POJK.03/2018") is the main step that has been taken by the government in regulating electronic-based banking activities. This is stated as a progressive step from the Financial Services Authority ("OJK") which plays an important role in providing digital banking services by commercial banks, especially to accommodate customer needs. (Reka Dewantara, 2022)

As regulated in POJK No. 12/POJK.03/2018, Electronic Banking Services are "services provided by the Bank for its customers to obtain information, communicate and carry out banking transactions via electronic media." Then, Digital Banking Services themselves are defined as "electronic banking services designed to optimize the use of customer data in order to provide services to customers that are faster, easier and according to their needs (*customer experience*) and can be accessed independently by customers, while still upholding security aspects."

Behind that, the existence of digital banking welcomes technological innovation which can be used as a forum for banks to channel their creations. Especially for the growth of banks which should offer a variety of new product choices in carrying out banking activities ranging from payments, fund transfers, to investments. The transformation that has occurred has improved the quality of banking

ISSN print 2086-6852 and ISSN Online 2598-5892

services, especially in creating opportunities for bank customers to obtain more information, communicate, register, open accounts, banking transactions and close accounts, including obtaining other information and transactions outside of banking products, including advice. finance (*financial advisory*), investment, electronic-based trading system transactions (*e-commerce*), and other needs. (Putera, 2020)

With these changes in banking facilities and methods, the need for a legal umbrella that can protect customers and banks also accompanies it in order to prevent or resolve problems that increasingly arise in the future. In order to provide legal protection for customers regarding obstacles and irregularities that occur in digital banking activities, Article 21 paragraph (1) POJK No. 12/POJK.03/2018 regulates that banks that provide electronic or digital banking services are obliged to uphold the principles of consumer protection as regulated by statutory provisions regarding consumer protection in the financial services sector.

Digital banking providing color in every financial activity of its customers. Apart from having convenience that can make customers feel benefited, this digital banking service is not free from gaps in the emergence of problems that will later be faced by banks. Every change will definitely give rise to new risks. In this case, these risks can be risks related to the bank's daily operations, as well as risks to the bank's reputation in the public eye. In banking transaction activities via digital services, it is not uncommon for legal problems to arise which can be detrimental to the parties. Legal problems that are often encountered through digital banking services relate to information system security. With these facts, the security factor is important and needs to be considered. A strong security system can support and streamline all service activities*digital banking*. (Hidayat, 2021)

In business relationships that exist between banks and customers, banks should prevent the occurrence of various risks by fulfilling obligations for banks to identify, authenticate and verify customer information and supporting documents. In order to comply with regulations issued by Bank Indonesia regarding the principle of knowing your customer, Bank Indonesia intends for banks under it to know the identity of customers as a form of anticipating various risks and of course forming the foundation for a strong security system defense. Also related to the application of the Prudential Principle in Banks (*prudential banking*) which is closely related to banking transactions, one effort to ensure that this principle can be implemented is to apply the Know Your Customer Principle. (Rahman, 2022)

In particular, the verification stage in digital banking is needed to measure customer truth and compatibility. The identity verification process should be carried out before carrying out financial

ISSN print 2086-6852 and ISSN Online 2598-5892

transactions. Generally, verification can be done face to face and without face to face. Currently, face-to-face verification methods can be carried out in several ways, namely: Directly (*face to face*); or Using bank-owned software with bank-owned hardware; or Using hardware belonging to customers and/or potential customers. Meanwhile, non-face-to-face verification is carried out using the bank's software with the bank's hardware or the customer's and/or prospective customer's hardware. The digital banking security models currently implemented through internet banking include:*Digital Certificates, One Time Password (*OTP*), Browser Protection, Virtual Keyboards, Device Registering, Completely Automated Public Turing test to tell Computers and Humans Apart (*CAPTCHA*), Short Message Service (*SMS*), Device Identification, Positive Identification, Pass-Phrase, dan Transaction Monitoring*. (You too, 2021)

Based on the description above, the actual emergence of various Digital Banks does not necessarily eliminate the possibility of mistakes or errors occurring in their operations, whether intentional or unintentional errors, one of which is deliberate error.*Fraud* and or*cybercrime* (as crimes that occur through or on computer networks on the internet) in the electronic services of this digitization,*Fraud* is a form of error that can be defined in various ways and is different in each field.*Fraud* in the financial services sector itself, it can take the form of irregularities, cheating, deception, and/or unlawful misuse for personal or group gain and/or legal entities which cause losses to other parties in the case of Digital Bank customers.

Shapes*fraud* and/or*cybercrime* which can cause losses to customers may arise either from the Bank or from other irresponsible parties. As a new entity, of course there are many possibilities for implementation ineffectiveness, operations that are not up to date, supervision that is still lax, and the level of compliance with crucial matters that is still not up to date, so there is a need for legal protection for customers who use and/or carry out their banking transactions through This Digital Bank. Losses caused by*fraud* and or*cybercrime* This is not a small loss and can be ignored, the increase in crime has caused many customers to experience it

2. RESEARCH METHOD

The type of method used in this research is the normative legal research method. The normative legal research method is a procedure for finding legal rules, legal principles and legal doctrines to answer the legal problems faced. (Marzuki, 2017) The approach used in this writing is the statutory approach or statute approach, namely an approach through the use of legislation and regulations and also paying attention to the hierarchy and principles in statutory regulations. (Achmad, 2015) Then, this research uses a conceptual approach (*conceptual approach*) because one

ISSN print 2086-6852 and ISSN Online 2598-5892

part of this research will begin by identifying existing doctrinal principles or views to then generate new ideas. This normative legal research is descriptive in nature as part of legal science activities to explain the law. Only facts are the primary legal material for explaining the law. Making decisions about law in the legal field. (Rahayu, 2020)

3. RESULTS AND DISCUSSION

Digital Banking Service Security System

The operation of digital banking services certainly creates various risks and new problems for customers and also the organizing bank. Currently, there are no statutory regulations that specifically regulate digital banking services. However, in its implementation it still refers to Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 ("Banking Law"). Organizing banks must continue to comply with the Banking Law in various aspects, starting from businesses in the form of commercial banks, implementing*prudential banking*, and protect customers' personal data.

In essence, technical supervision and guidance of banking operations as regulated in Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 is carried out by Bank Indonesia. According to Law Number 23 of 1999 concerning Bank Indonesia ("BI Law"), the banking supervision function which was previously the authority of Bank Indonesia will be transferred to a special institution, namely the Financial Services Supervisory Agency which was formed in 2002, this institution is based on law to then supervise business activities carried out by financial institutions operating in Indonesia. (Wahjusaputri, 2018) However, on December 31 2013, Bank Indonesia and the Financial Services Authority signed a Minutes of Handover (BAST) on the transfer of bank regulatory and supervisory functions from Bank Indonesia to the Financial Services Authority ("OJK"). So with this, the authority to regulate and supervise banks by the OJK includes: determining licensing procedures (*right to license*); set conditions (*right to regulate*); supervise banks directly and indirectly (*on-site and off-site supervision*); impose sanctions (*right to impose sanction*); carry out an investigation (*right to investigate*); and carry out consumer protection (*right to protect*). (Wahjusaputri, 2018)

Likewise for banks that provide digital banking services, based on POJK No. 12/POJK.03/2018, "Banks that provide Electronic Banking Services or Digital Banking Services, are required to implement risk management, prudential principles, and fulfill the provisions as regulated by statutory regulations." Basically, banks that provide technology and information-based banking services are obliged to prioritize security aspects. This is clearly stipulated that "Banks are obliged to

ISSN print 2086-6852 and ISSN Online 2598-5892

apply the principles of controlling the security of customer data and transactions from Electronic Banking Services in every electronic system used by the Bank".

In general, security is a condition that frees oneself from fear or anxiety. Information security is a process that is deliberately designed and implemented to protect information from unauthorized access, use or misuse. In the banking service system, security is a fundamental factor, especially in generating a sense of trust from customers and the public in the good name of the organizing bank. This digital banking service has a very wide network and has provided effectiveness for its users and administrators. However, new risks have emerged that threaten the security of using this banking service. Therefore, protection is needed against various types of security attacks. Based on Budi Rahardjo's view, in the security system planning process it is necessary to evaluate and maintain 5 (five) basic components, including the following: (Rahardjo, 2017)

1. *Confidentiality. Confidentiality* or confidentiality in a security system is a factor that can only be accessed by authorized people. Therefore, banks providing digital banking services need to carry out regular checks so that information kept confidential by customers cannot be accessed by unauthorized parties;
2. *Integrity. Integrity* is that changes are not permitted if they are not permitted by the entitled party. This is related to preventing parties who attempt to modify information that they do not have the right to. In digital banking services, this component is where authorization from the customer is required;
3. *Availability. Availability* is that the necessary information can be used, or in other words the information can be accessed when needed. If system*not available*, then it can cause losses. As is*availability*, the organizing bank can prevent control of information by unauthorized parties. This component provides assurance that the service system can be accessed by authenticated customers whenever the information is needed;
4. *Authentication. Authentication* generally used as an opening route for providing information. This process is used to prove that someone is who they claim to be. Generally, customers use this authentication aspect for their ATMs or accounts. Where to access the ATM or account you have to go through an authentication process that only you know. Like using userid,*password*, or PIN. Currently, authentication has developed with more sophisticated programs using only fingerprints or*facial recognition* owner customers; And
5. *Non-repudiation. Non-repudiation* functions to make customers unable to deny that they have made a transaction. Generally, it is done with*digital signature* or by telephone.

ISSN print 2086-6852 and ISSN Online 2598-5892

In order to provide maximum security aspects, coordination is required between the organizing bank and user customers. This is intended to maintain the security system in transactions in digital banking services. The following is a system that can be provided by the bank to maintain the security of customer use of services:

1. System*Cryptography*

This system is generally known as a password system which uses numbers as keys. This system is intended to protect customer financial information; And

2. System*Firewall*

This system is used to prevent unapproved parties from entering protected areas or in this case customer financial information. System*firewall* will hold back intruders with more complex options.

In Article 15 paragraph (5) POJK Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks ("POJK 12/POJK.03/2018"), banking service providers are obliged to implement 2FA in a transaction. The bank must provide at least 2 (two) layers of security either based on the partnership agreement or on behalf of the bank itself. Then, the form of 2FA security must be in accordance with the plan for providing digital banking services by Commercial Banks as stated in Appendix A POJK 12/POJK.03/2018 Number 6 letter (A). Banks must determine the form of 2FA that will be used as a security layer for their services. It needs to be underlined that what is mandatory to implement according to POJK 12/POJK.03/2018 is the use of 2FA. However, the form is free. Among them are such as*face recognition*, OTP code, token, independent data entry, and so on. So, if the OTP code is used as an application of 2FA, this is very permissible. In fact, currently OTP codes are very common and easy to find on almost all digital banking services.

The Bank's obligations exist from the initial stage, namely planning, and not when the service is already running. For example, BNI wants to create BNI*Mobile Banking*. When you want to apply for permission to launch*Mobile Banking* Accordingly, BNI must explain what 2FA will be used in BNI*Mobile Banking* along with procedures, rules, security, and so on. When there are changes, for example adding features to access BNI Mobile Banking, BNI must apply for permission again. This is principled because it is related to consumer protection.

Responsibility for Electronic Transactions of Digital Banking Services

Behind the convenience obtained from using digital banking services, of course there are risks that can harm customers. Many legal violations were found, especially those related to customer personal data. Moreover, it is not uncommon to find customers who suffer financial losses due to the actions of irresponsible parties (technology and information criminals) which ultimately requires the

ISSN print 2086-6852 and ISSN Online 2598-5892

banking industry to build a very high level of security in order to maintain trust and reputation in the community that digital banking services provide. it is safe to use. (Raditio, 2014) In this regard, legal protection is needed for customers using digital banking services in order to protect customers' rights as consumers in banking services.

The Banking Law should not regulate provisions regarding legal protection for bank customers in detail. There is a little explanation that states that banks must provide information about risks arising from transactions carried out by customers through the bank, but there is no understanding that explains how banks must protect customers' interests as a whole. The government considers that customers are consumers in the banking industry, so the regulations are indirectly included in the Consumer Protection Law.

On the continuity of the payment process in the Digitalization Process in*Mobile Banking* For legal protection for customers, regulations regarding legal protection for user customers refer to Bank Indonesia regulations. Where the organizing bank is required to provide a reliable system and be accompanied by the provision of facilities that make it easier for consumers to obtain information. In fact, there is Chapter IV specifically to require banks to carry out outreach and education regarding the implementation of consumer protection. This regulation also regulates the complaint mechanism that must be provided to consumers, which includes receiving complaints, handling and resolving complaints, and monitoring them. The Organizing Bank is also required to follow up and resolve complaints submitted by consumers.

More specifically, in providing digital banking services, the OJK also plays a role, as the authorized authority to carry out regulatory and supervisory functions in pursing regulations regarding legal protection for bank customers. This action is of course based on the OJK Law which states that the OJK provides consumer complaint services in the financial services sector and "further provisions regarding consumer and public protection are regulated by OJK Regulations ("POJK")."108 On the basis of these provisions, the OJK issuedBOY regarding consumer protection in the banking sector, including POJK No. 6 /POJK.07/2022 Concerning Consumer and Community Protection in the Financial Services Sector which states that "consumer protection in the financial services sector aims to create a reliable consumer protection system, increase consumer empowerment, and raise awareness of financial services business actors regarding the importance of consumer protection so as to increase public trust."

OJK also issued provisions regarding consumer protection, namely POJK No. 18/POJK.07/2018 concerning Consumer Complaint Services in the Financial Services Sector. The outline of this regulation is a provision which states that if the complaint service does not reach the

ISSN print 2086-6852 and ISSN Online 2598-5892

midpoint, then the problem can be resolved by filing a lawsuit through the courts or Alternative Dispute Resolution Institutions determined by the List of Alternative Dispute Resolution Institutions (non-court channels) that have been previously determined by OJK.

For problems such as fraud, embezzlement and other criminal acts, criminal justice charges can be filed. In relation to digital banking services, POJK no. 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks has its own chapter, namely Chapter V, which regulates customer protection. Article 21 paragraph (1) regulates that "banks providing digital banking services are required to implement consumer protection principles as regulated inBOY regarding consumer protection in the financial services sector." Banks are also required to "provide customer inquiry and/or complaint services that operate 24 (twenty four) hours a day."

Based on the description above, in carrying out digital banking services, banks are required to implement effective risk management and legal protection. This is very important for operational continuity and even the reputation of the organizing bank itself. When providing digital banking services, customers generally use them to make online transactions, transfer funds to other accounts or shop on e-commerce, for example. This activity is classified as an electronic transaction. According to the ITE Law, business actors who offer products through electronic systems must provide complete and correct information regarding contract terms, manufacturers and the products offered. Knowing this, banks that act as business actors must provide very clear and detailed information regarding the flow of use of services and the risks that may occur, so that customers can carry out electronic transactions while upholding transaction security for themselves. Because basically, if using digital banking services requires customer personal data information via electronic media, this must still be done with the consent of the person concerned. Responsibility for the legal consequences that arise when carrying out electronic transactions depends on who carries out the transaction, this is divided into several conditions: (Putra, 2020)

1. If the losses experienced by customers using digital banking services occur due to their own mistakes, then the legal consequences in carrying out electronic transactions are the responsibility of the parties to the transaction (customers). In other words, customers cannot submit claims to the bank and the bank does not have to provide compensation, but the bank still needs to provide assistance for solutions experienced by customers;
2. If losses occur and are carried out through the granting of power of attorney, all legal consequences in carrying out electronic transactions through digital banking services are the responsibility of the power of attorney (Pratiwi, 2018); And

ISSN print 2086-6852 and ISSN Online 2598-5892

3. When done through an electronic agent, all legal consequences in the implementation of electronic transactions become the responsibility of the electronic agent."

Then, the ITE Law also provides an opportunity for parties who feel their rights have been harmed to file a lawsuit, as stated that "everyone can file a lawsuit against a party that operates an electronic system and/or uses information technology that causes harm." Apart from that, through court, the parties also have the option to resolve their disputes with other alternative dispute resolution institutions in accordance with statutory provisions such as arbitration. For this reason, the bank as the provider of digital banking services will also impose an obligation on customers to be more alert, thorough and careful in using the services it offers.

Law Number 27 of 2022 concerning Protection of personal data also regulates criminal provisions in the event of fraud in personal data and as preventive protection for customers, namely where there is an unlawful act in obtaining or collecting personal data with the aim of benefiting oneself. be sentenced to imprisonment for 5 (five) years and/or a fine of a maximum of Rp. 5,000,000,000.00 (five billion rupiah). Acts of disclosing customer personal data are subject to imprisonment for a maximum of 4 (four) years and a fine of a maximum of Rp. 4,000,000. ,000.00 (four billion rupiah), using customer personal data unlawfully is subject to a maximum penalty of 5 (five) years and a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah). And the act of falsifying personal data for unlawful use will be punishable by a maximum of 6 (six) years and/or a maximum fine of IDR 6.0OO. 000,000.00 (six billion rupiah).

In terms of crime*fraud* carried out on behalf of the Digital Bank, the sanctions imposed are only administrative sanctions, namely in the form of a fine of 10 (ten) times the maximum criminal fine with additional sanctions such as confiscation of profits, freezing of business activities, prohibition of certain actions, closure of business premises, carrying out neglected obligations, payment of compensation, revocation of license and/or dissolution of the digital bank.

Several crucial elements in this theory are contained in the purpose of these regulations, such as that the theory is an effort to organize interests, where the government and the authorities authorized to make these regulations clearly provide a division of power for each institution in making regulations in accordance with its authority. This division is carried out by limiting certain interests in an organized manner so as to be able to create a good legal protection system for customers. Another element of this theory is that the community, in this case the customer, can enjoy the legal rights that are properly owned and given to them. Realization of legal protection for customers*Fraud* and phishing that occurs in Digital Bank transaction activities can be seen from how the government and

ISSN print 2086-6852 and ISSN Online 2598-5892

authorities in the Financial Services sector are trying to regulate and limit various interests and powers so that they do not collide with each other and are optimally organized.

Efforts to protect customers are also guaranteed to be realized by seeing how the government and competent authorities enforce sanctions provisions for anyone who violates these provisions as one of the preventive measures for prevention and control. However, in its application and implementation, several factors and aspects are still found that are not implemented in accordance with the regulations that regulate it, where in the event of fraud, the authorized institutions in the financial services sector are too lax in thoroughly investigating the perpetrators, so this results in no deterrent effect. for the perpetrator and causes the crime to continue and never stop and customers will always be at risk of loss.

The Urgency of Improving Cybersecurity in the Digitalization Process in Mobile Banking for Legal Protection of Customers

The demands of the times ultimately encourage the financial sector to provide fast, efficient and safe services, giving birth to new business models, especially banking institutions. Banks as intermediary institutions need to participate in innovation in accordance with developments and demands of the business environment in order to optimize their contribution to national economic stability and growth. This is in accordance with the Bank's function, namely collecting funds and channeling public funds to improve the standard of living of the wider community. The use of Information Technology (IT) in banking operational activities can be reflected in non-face to face and paperless document systems that utilize certain hardware and software. The services provided by banks today have also entered the digitalization era, such as providing payment services via*Automated Teller Machine* (ATM) *mobile banking*, *internet banking*, *Quick Response Code Indonesia Standard* (QRIS) and the use of IT to support banking operational activities.

One of them is digital transformation in carrying out the principle of getting to know customers from previously based on conventional or*Customer Due Diligence* (CDD) be*Customer Due Diligence* electronically. The legislation itself does not differentiate between the definition of conventional CDD and electronic CDD. Therefore, the meaning still refers to what is meant by customer due diligence or CDD as defined in Article 1 number 11 POJK No. 23/POJK.01/2019 concerning Amendments to POJK No. 12/01/2017 concerning Implementation of the Anti-Money Laundering and Prevention of Terrorism Financing Program in the Financial Services Sector, namely "Identification, verification and monitoring activities carried out by the Bank to ensure transactions match the profile, characteristics and/or transaction patterns of customers or prospective customers ."

ISSN print 2086-6852 and ISSN Online 2598-5892

Electronic CDD is based on technology*artificial intelligence* is a human creation that is not immune from cyber risks. One example of cyber risk that is a challenge for the electronic CDD process includes leaks of customer personal data information, identity theft, account takeover attacks, and deepfake technology which allows someone to impersonate a legitimate customer. Like the identification and verification process in electronic CDDs, deepfakes are the result of programming*artificial intelligence* with an algorithm that is able to manipulate faces in photos or videos to manipulate a person's voice to resemble someone else's, where the results will be very accurate and detailed like the original. (Westerlund, 2018)

Based on this, basically Digital Banks are classified as financial services sector entities that carry out banking activities by utilizing sophisticated technology where all banking access and procedures are carried out using the internet network, basically Digital Banks are a form of digitalization of conventional banks that previously existed in Indonesia with the aim of attracting more markets to use bank products and services and by offering convenience so that they can be accessed and reached by anyone from anywhere. However, as time goes by digital and technological developments encourage Digital Banks to form various services that are more integrated compared to conventional banks where there are several products and/or digital services which are new forms of products and services and are original to Digital Bank only, including products and/or services developed by Digital Bank.

With various intensive developments of new information systems, products and services developing in this Digital Bank, it creates a lot of great potential that is almost unlimited, but the rapidly developing technology also directly poses challenges for regulators, namely the competent authorities in the sector, business players in this is the Digital Bank itself, as well as the public or customers. This certainly raises the challenge of finding ways to regulate digital banking activities with these innovations and how to create digital technology by emphasizing more benefits for all parties and by paying attention to risk factors for failure and dangers that could be detrimental. In other words, this innovation is double-edged, where the advantages and disadvantages are equally great. (Jon Truby, 2020)

In implementing this technology, the competent authorities in the financial services sector must be able to pay attention to factors that are profitable and can take place safely and beneficially for all parties. Therefore, it is necessary to look for new instruments for regulating digital technology that can answer the interests of all parties. One of the tools used for regulation is the Regulatory Sandbox, where this regulatory tool model aims to encourage innovation activities by allowing business entities to test offers provided to customers to be safe and provides an example of a shift

ISSN print 2086-6852 and ISSN Online 2598-5892

from traditional regulatory approaches and represents an effort to embrace the principles of proactive, dynamic and responsive regulation. This Regulatory Sandbox regulatory tool model was first launched in the UK in 2016, at which time this model was successfully implemented in countries around the world such as Singapore, Australia, UAE, USA and several other European Union countries. (Elizaveta Gromova, 2020)

One of the impacts of the widespread use of technology and digital media is weaknesses and/or cyber security which causes many losses, so there is great hope that this regulation can be a support for innovators to carry out experiments in technology products and/or services and test them directly in the market on customers and It is also hoped that it will be able to reduce the impact of the absence of regulation in the digital economy. Scheme on*Regulatory Sandbox* This is to enable testing of Digital Bank products and/or services before entering or being applied to customers on a large scale, where the test results can also be used as a study and evaluation for the regulatory framework related to the suitability and security of electronic and digital systems. (Patrick Bernard Washington, 2022)

The aim of establishing and implementing the Regulatory Sandbox is basically to create an adequate legal basis for regulation of the digital era by state institutions and authorities in the financial services sector who have a role in further technological development, where this regulation is also intended as a modern effort.*Smart Regulation, Good Governance,* and *Agile Governance* where regulations and government management must be flexible and sensitive to existing transformation processes and based on new methods and models. Where this regulatory concept is based on the aim of rapid development and intelligent regulatory tools that support digital technology innovation. (Faykiss, 2018)

Regulatory sandbox It is also a form of legal umbrella in dealing with the spread of digital technology which causes the emergence of new ways in the means of digital applications or services, by inheriting international or foreign experience in digital technology settings which makes it possible to define several general approaches in one setting. According to several experts, implementing this regulatory approach is a difficult matter for the competent authorities in the financial services sector, but considering the need to strike a balance between freedom of innovation and the risks and dangers that come from the unregulated use of digital technology innovations, this has prompted the government to look for an approach new regulations regarding innovation.

There is one type of approach in forming this regulation, namely "*Cautious Permissiveness Through Flexibility and Forbearance*" where in this approach the implementation of regulations is carried out by involving the softening or relaxation of existing rules in certain contexts, where this

ISSN print 2086-6852 and ISSN Online 2598-5892

approach is widespread throughout the world and is applied when encouraging the development of innovation. Whereas this approach is aimed at establishing new regulatory tools for technological innovation, when looking for new regulatory tools modern countries consider tools such as deregulation, co-regulation, risk-based regulation, or compliance-based regulatory tools.

Apart from that, the Bank cannot turn a blind eye to cases of technology that continues to develop, such as*deepfake* which has occurred, especially in the verification process*mobile banking*. Banks need to consider misuse of technology*deepface* as well as the development of AIR as a form of operational risk that may be faced. Therefore, Banks are mandated to always implement the principles of good IT governance and risk management. Furthermore, banks are not only required to have good IT infrastructure. However, it is also necessary to maintain the security of its electronic systems and have the ability to detect and recover after a cyber incident occurs. POJK PTI has regulated matters that banks must pay attention to and prepare for implementing IT.

So banks are obliged to maintain their IT cyber resilience by identifying assets, threats and vulnerabilities. Furthermore, Banks are also required to carry out asset protection, cyber incident detection, and cyber incident response and recovery. Each of these processes has its own function in maintaining cyber resilience. For example, in the process of identifying assets, threats and vulnerabilities, the Bank will carry out an inventory and assessment of the hardware, software, network and infrastructure it owns. Later, the Bank will carry out cyber security testing on these IT assets. Furthermore, Banks are required to implement security controls on IT assets based on the results of previously conducted cyber security tests. Another example, in the cyber incident detection process, the Bank needs to monitor suspicious activity and ensure that the Bank's IT system can detect suspicious activity in a timely manner. Furthermore, the Bank needs to ensure that the handling of cyber incidents is effective so that it can prevent disruption to the Bank's overall operations

4. CONCLUSION

As time progresses, there are more and more opportunities for people to abuse this convenience in order to make things easier for themselves. Indeed, there must be preventive methods for banks, related authorities and also customers to maintain usage*mobile banking* which is a digital banking service. Realization of legal protection for customers*fraud* or*cybercrime* What happens in Digital Bank transaction activities can be seen from how the government and authorities in the Financial Services sector attempt to regulate and limit various interests and powers so that they do not collide with each other and are optimally organized. Efforts to protect customers are realized through the Government and Authorities who have the authority to enforce Sanction provisions for anyone

ISSN print 2086-6852 and ISSN Online 2598-5892

who violates these provisions as one of the preventive measures for prevention and control. However, in its application and implementation, several factors and aspects are still found that are not implemented in accordance with the regulations that regulate it, which in the event that this occurs*fraud* or*cybercrime* by Internal Banks that carry out Digitalization themselves, as well as Institutions authorized in the financial services sector are too lax in terms of thoroughly investigating the perpetrators, so that this results in no deterrent effect for the perpetrators and causes these crimes to continue and never stop and customers will always remain threatened with loss.

In practice, due to the many risks that arise from providing Mobile Banking services, these risks are still often realized. However, Commercial Banks are obliged to carry out their business activities with caution and implementation*Good Corporate Governance*, Risk Management and Consumer Protection will be better prepared to face various risks arising from the provision of Mobile Banking services. Commercial Banks are expected to continuously implement the Prudential Principle and pay attention*Good Corporate Governance*, Risk Management, and Consumer Protection in providing services*Mobile Banking* because if this is not done then the loss will be felt not only by service users but the Commercial Bank itself as the service provider, as can be seen in the case examples in the decision, not only service users will experience material losses but the Commercial Bank's reputation can also be tarnished by the occurrence of the incident. like that.

Mechanism of the trial system*Regulatory Sandbox* This allows innovators to receive various guidance from the competent authority regarding their products and/or services that contain digital financial innovation, generally the competent authority can provide direction and interpretation regarding legal requirements where the provisions of the law that regulates whether a digital innovation is appropriate or not regulated, it is possible that with this process the competent authority can also provide an overview of developments and opportunities to develop digital financial innovation to be more advanced. It is also possible for innovators to receive suggestions from authorities in terms of developing global innovation where there are innovation centers which generally only have connections with competent authorities, so that indirectly this trial process also provides great opportunities for innovators to collaborate in developing its innovations as widely as possible, even to the international level.

In terms of digital finance, Indonesia does not yet have related laws, but the adoption of regulations related to the Regulatory Sandbox is a form of government effort in terms of readiness to create a legal framework related to the implementation of digital financial products and/or services by Digital Banks, where digital technology is improving. which has a big impact on the Indonesian

ISSN print 2086-6852 and ISSN Online 2598-5892

economy. Where the trial system in this regulation is expected to help innovators, in this case Digital Banks, can be encouraged to develop innovation continuously, feasible and safe.

REFERENCE

Abdullah, Thamrin and Sintha Wahjusaputri, (2018). *Banks and Financial Institutions*, Edition 2, (Jakarta: Mitra Wacana Media.

Adiguna, Vania Keryn.(2021), "Judicial Review of Banking Transactions Via Internet Banking in Manado,"*Privacy Law* IX, no. 4, (April 2021): 39, https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33343

Baidlowi, Rully and Arief Rahman.(2022). "Implementation of the Prudential Principle in Online-Based Credit Agreements".*Private Law* 2, no. 3, (October 2022): 657-665. https://doi.org/10.29303/prlw.v2i3.1562

Dewantara, Reka and Hany AyundaMernisi Cytorus.(2022). "Re-Evaluation of the Establishment of Digital Banks in Indonesia: Paradigms, Concepts and Regulations."*Truth and Justice* 8, no. 2 (Desember 2022): 493-513, https://doi.org/10.25123/vej.v8i2.5433.

Emanuella, Claudia Saymindo. (2021). "Central Bank Digital Currency (CBDC) as a Payment Tool in Indonesia", Vol. 4*JuristDiction* 4, no. 6, (2021): 2253, https://doi.org/10.20473/jd.v4i6.31845.

Faykiss Peter, dkk, (2018). "Regulatory Tools to Encourage FinTech Innovations: The Innovation Hub and Regulatory Sandbox in International Practice)", Financial and Economics Review 17, no. 2, (2018): 68-69, https://doi.org/10.25201/FER.17.2.4367.

Fure, Joey Allen, (2016). "Functions of Banks as Financial Institutions in Indonesia According to Law Number 10 of 1998 concerning Banking."*Criminal Law* 5, no. 4 (July 2016): 116, https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/13122.

Gromova, Elizaveta.(2020). "Regulatory Sandboxes (Experimental Legal Regimes) For Digital Innovation in BRICS", BRICS Law Journal 7, no. 2 (2020):10-36, https://doi.org/10.21684/2412-2343-2020-7-2-10-36

Huda, Miftakhul (2021). "The Role of the Financial Services Authority in Supervising Banking Health in Indonesia." Salimiya:*Journal of Islamic Religious Studies* 2, no. 3 (September 2021): 61-77, https://ejournal.iaifa.ac.id/index.php/salimiya/article/view/385.

Kurnianingsih, Asih and Muhammad Rifqi Hidayat, (2021). "Transaction Security Factors and Risk Perceptions in Deciding to Use Banking Services Mediated by Customer Trust."*Journal of Management and Retail* 1, no. 02 (2021): 179-200, http://ejournal.lppm-unbaja.ac.id/index.php/jumareta/article/download/1579/1348.

Putera, Andika Persada (2020).*Banking Law: Analysis of Principles, Products, Risks and Risk Management in Banking*. Surabaya:Scopindo Library Media.

ISSN print 2086-6852 and ISSN Online 2598-5892

Mutiasari, Annisa Indah, (2020). "Development of the Banking Industry in the Digital Era."*Journal of Business Economics and Entrepreneurship* 9, no. 2 (August 2020): 32-41, https://doi.org/10.47942/iab.v9i2.541.

Marzuki, Peter Mahmud, (2017).*Legal Research*, 13th printing, (Jakarta: Kencana Prenada Media Group, 2017

Rahayu, (2020). Derita Prapti.*Legal Research Methods.* Yogyakarta: Thafa Media.

Rahardjo,(2017). Budi.*Information Security*, Bandung: PT Insan Infonesia.
Raditio, (20145), Resa.*Legal Aspects of Electronic Transactions*, Jakarta: Graha Ilmu.

Son, I. Made Aditya Matara, (2020). "Bank's Legal Responsibility towards Customers in the Event of Transaction Failure on the Mobile Banking System."*Kertha Wicaksana* 14, no. 2 (July 2020): 132-138, https://doi.org/10.22225/kw.14.2.2020.132-138.

Santoso, Agus, and Dyah Pratiwi (2018). "Responsibilities of Electronic Banking System Operators in Electronic Transaction Activities Post Law Number 11 of 2008 concerning Information and Electronic Transactions." Indonesian Legislation Journal 5, no. 4 (2018): 74-88, https://doi.org/10.54629/jli.v5i4.307.

Tarigan, Herdian Ayu Andreana Beru and Darminto Hartono Paulus, (2019), "Legal Protection of Customers for Providing Digital Banking Services,"*Journal of Indonesian Legal Development* 1, no. 3, (September 2019): 295, https://doi.org/10.14710/jphi.v1i3.294-307.

Truby, Jon, (2020). "Fintech and the city: Sandbox 2.0 policy and regulatory reform proposals." International Review of Law, Computers & Technology 34, no. 3 (November 2020): 277-309, https://doi.org/10.1080/13600869.2018.1546542.

Westerlund, Mika, (2018). "The Emergence of Deepfake Technology: A Review," Technology Innovation Management Review 9, no. 11, (November, 2018): 40, http://doi.org/10.22215/timreview/1282

Washington, (2022), Patrick Bernard, Shafiq Ur Rehman, dan Ernesto Lee. "Nexus between regulatory sandbox and performance of digital banks—A study on UK digital banks." Journal of Risk and Financial Management 15, no .12 (December 2022): 610, https://doi.org/10.3390/jrfm15120610.