Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 5733-5744*

Research Article

Law Enforcement and Prevention of Banking Criminal Actions in Indonesia

Andi Aina Ilmih[a], Edi Ribut Harwanto[b]

[a]Student of the Doctor of Law Program at Diponegoro University Semarang-Lecturer at the Law Faculty of Sultan Agung Islamic University, andiaina@unissula.ac.id/andinazuldina@gmail.com
[b]Siirt Head of the Laboratory of Law Faculty, Muhamadiyah Metro University, Advocate-Lecturer in Economic Criminal and Intellectual Property Rights at the Law Faculty of Muhammadiyah Metro University, edi.rharwanto@yahoo.com/edilaw5863@gmail.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Cyber Crime in the digital era is an extraordinary crime that has attacked the Indonesian banking sector with various modes through digital technology facilities. There are third parties outside the bank hackers, and many also involve people within the bank themselves with various modus operandi using embezzlement in their positions to manipulate digital financial reports or fake accounts, fake calls on behalf of the bank to take customer money with illegal proceedings. This study uses a post-positivism paradigm. The results of the author's research, the forms of crime that have occurred so far are various modes of crime committed by bank employees, third parties with various modes of crime. The conclusion is that there needs to be an increase and awareness that everyone in facing this era must have a new awareness, in this digital era they must be more aware of protecting data and always protecting it. Because there are risks that must be regulated to provide a sense of security for customers and continue to enforce the law according to the Banking Law, the Information and Telecommunication Law, the OJK Law and the Corruption Crime Law. Technological developments are a challenge for banks to improve security in transactions in order to ensure predictableness and preciseness for customer fund protection.

Keywords: fictitious transactions, embezzlement in office, card tapping crime, skimming, investment security, cyber crime

1. Introduction

A criminal act is an act for which the perpetrator is subject to criminal penalties based on law. The elements of a criminal act are the subject (the perpetrator) and the form of positive good deeds, namely committing an act, or negative, namely not committing an obligatory act. Basically, criminal provisions must cover the entire penal system. According to Nils Jareborg, the entire structure of the penal system is a matter of criminalization; formulation of criminal acts, problems of conviction or imposition of sanctions and problems of the implementation of criminal or criminal law sanctions (execution of punishment). In reality, we will look at the implementation of criminal law enforcement and criminal sanctions against banking crimes in Indonesia. Banking crimes are always related to public funds deposited in banks, therefore this harmful banking crime involves the interests of various parties, both the bank itself as a business entity as well as a fund depositing customer, the banking system, the banking authority, the government and the wider community. Various modes of crime are committed by bank employees, third parties with various modes of crime. In this case, there are minor people who are blind to the law, usually resolved by means of mediation or out of court settlement. Based on observations of empirical reality, it is known that various types of banking crimes exist, such as card tapping crimes; criminals will install a device in the form of a stick on the ATM machine so that customers cannot make transactions. When a customer is confused, the perpetrator acts by pretending to be helpful. At that time, the perpetrator memorized the card PIN. The conspirators will also exchange the customer's ATM card, so that transactions by withdrawing customer money can be carried out. Another familiar form of banking crime is skimming. The camera will be attached to the card holder on the ATM machine. From there the perpetrator memorized the PIN and duplicated the card. Recently there were reports of many customers, how come their money was lost; where is the responsibility of the bank? Safe or not? We can see from two sides, banks continue to improve the security of their systems and customers must also know the rules of the game. Director of Digital IT & Operation of PT Bank Rakyat Indonesia (Persero) Tbk. Indra Utoyo, said the threat of digital crime in the banking system is very dynamic, so security improvements must be made. BRI this year provides funds worth IDR 3.7 trillion for digital investment capital costs. The capital costs will be used for infrastructure modernization to increase security. Other banking criminal cases, the theft of Central Java Bank, MayBank and several other banks in Indonesia.

The use of the terms banking crime (tipibank) and banking crime does not yet have a common opinion. When viewed from a juridical perspective, none of the laws and regulations provide an understanding of banking crime.

In terminology, the term ‘tipibank’ is different from criminal acts in the banking sector. Criminal acts in the banking sector have a broader definition, namely all types of illegal acts related to activities in running a bank business. So that these acts can be treated with regulations governing banking activities which contain criminal provisions as well as general / special Criminal law regulations, as long as there are no Criminal Law regulations specifically made to threaten and punish these acts. This means that a criminal act in the banking sector involves an act related to banking and is punishable by crime, even though it is regulated in other regulations, or besides being an act that violates the provisions of the Banking Law and the Sharia Banking Law, is also an act that violates the provisions outside. The Banking Law and the Sharia Banking Law which are subject to sanctions based on, among others, the Criminal Code (KUHP), the Corruption Crime Law, the Money Laundering Law, the act is related to the activities of running a bank business such as money laundering and corruption involving banks. In Law No. 10 of 2004 Sub C.3 No 85, contains general guidelines on the preparation of criminal provisions in statutory regulations, which contain formulas that state the imposition of criminal offenses against provisions containing norms of prohibitions or orders. The essence of this is that the criminal provisions contain the formulation of provisions containing norms of prohibitions or orders and provisions regarding the imposition of sanctions. With this, it means that banking criminal acts are regulated in the formulation of specific criminal provisions.

Meanwhile, ‘tipibank’ is more focused on prohibited acts, punishable by crimes specifically contained in the Banking Law and the Sharia Banking Law. The definition of ‘tipibank’ is a criminal act that fulfills the elements as referred to in Article 46 to Article 50A of the Banking Law or Article 59 to Article 66 of the Sharia Banking Law. Considering that the formulation of articles in the Banking Law and the Sharia Banking Act have many similarities, this paper intends to describe 'tipibank' as referred to in the Banking Law.

Legislation related to banking begins with Act No. 14 of 1967 concerning Banking Principles. Subsequently, in its development this Law was replaced by Act No.7 of 1992 concerning Banking as amended by Act No.10 of 1998 (Banking Law). With the need of the Indonesian people for sharia banking services that have specificities compared to conventional banking, the issuance of Law no. 21 of 2008 concerning Islamic Banking (Sharia Banking Law). The scope of ‘tipibank’ contained in the Banking Law and the Sharia Banking Act are:

a. Criminal acts related to licensing;
b. Criminal acts relating to bank secrecy;
c. Criminal acts related to bank supervision;
d. Criminal acts related to bank business activities;
e. Criminal acts related to affiliated parties;
f. Criminal acts relating to shareholders;
g. Criminal acts are related to compliance with the provisions.

The Banking Law distinguishes criminal sanctions into two forms, namely crime and offense. Violation of Position can only be committed by someone who has a position or position as a civil servant. The status of a person's civil servant is essential to categorize a violation as a violation of position. This is, if there is a banking crime (Tipibank) where the bank is a state-owned bank or a private bank that runs bank operations using loans or investment of state money as investment capital and / or other programs where the source of the bank's funds comes from the Expenditure Budget. State Expenditure (APBN) and Regional Expenditure Budget (APBD). In the Banking Law, the category of crime consists of seven articles, namely Articles 46, 47, 47A, 48 paragraphs (1), 49, 50, and Article 50A. Meanwhile, tipibank with a category of offense with a lighter criminal sanction than a crime classified as a crime, consists of one article, namely Article 48 paragraph (2). The classification of tipibank into crime is based on the imposition of the threat of punishment that is heavier than the offense. This is because banks are institutions that deposit funds entrusted by the public to them, so it is necessary to avoid actions that can damage public trust in the bank, which in effect will also harm the bank and the public. The Sharia Banking Act does not distinguish between bank type sanctions and lists them into eight articles, namely Articles 59 to 66.

2. Research Method

This study uses a post-positivism paradigm. The post-positivism paradigm wants to prove that everything is based on reality that can be built based on experience, observation, researchers are neutral towards the object of research. Even though researchers who hold this paradigm, still have to be neutral towards the object of research, which only examines what actually happens from things that seem certain. The post-positivism paradigm, ontologically, conceptualizes reality as it is, but it is realized that in fact many factors influence that reality. Consequently, ontologically, the post-positivism paradigm conceptualizes law as a set of regulations that apply in society whose enforcement will influence legal, economic, political, cultural and other factors. Epistemologically,

the researcher sits impersonal, separate from the object of research. The position of the researcher towards the research object is neutral and impartial. Post-positivism uses the principle of triangulation using various types of data sources and research approaches. Post-positivism adherents tend to use mixed methods (quantitative and qualitative) in conducting research. Mixed methods are considered to have the ability to provide integrated and inclusive understanding and results in research.

3. Result And Discussion

A. Banking Crimes Related to Licensing

The banking industry is known as a heavily regulated industry. To run a bank business requires a license from Bank Indonesia (currently OJK) as a regulator with strict requirements, as stated in Article 161 of the Banking Law, namely: "(1) Every party conducting activities:

1. Article 16 of the Banking Law is analogous to Article 5 paragraph (1) and Article 22 of the Sharia Banking Law. in the form of deposits, it is necessary to first obtain a business license as a Commercial Bank or Rural Bank from the Management of Bank Indonesia, unless the activity of raising funds from the public is regulated by a separate Law. raise funds from the community.

2. To obtain a business license for a Commercial Bank and Rural Bank as referred to in paragraph (1), the following requirements must be met at least:

a. organizational structure and management;

b. capital;

c. ownership;

d. expertise in Banking;

e. work plan eligibility.

3. he requirements and procedures for bank licensing as referred to in paragraph (2) shall be stipulated by Bank Indonesia".

A party conducting bank business activities prior to obtaining a license from Bank Indonesia (currently OJK) is categorized as a criminal offense. This crime is known as the crime of "black bank." Any party that collects funds from the public in the form of deposits without a business license from the Head of Bank Indonesia (currently the Chairman of the OJK) will be subject to serious criminal sanctions for "illegal bank". The threat of punishment can even be imposed on the corporation by suing the party who gave the order or its leader. This provision indicates the need for permission from the Bank Indonesia Management (currently the OJK Chair) for public fundraising activities, because it is closely related to the issue of monitoring these activities by Bank Indonesia (currently OJK). This provision is intended to protect public funds, because the activity of collecting funds from the public by anyone is basically an activity that needs to be supervised, considering that these activities are related to the interests of the community whose funds are deposited with the party that collects the funds.

Therefore, activities to collect funds from the public in the form of deposits can only be carried out by parties who have obtained a business license as a Commercial Bank or People's Credit Bank from the Management of Bank Indonesia (currently the Chairman of the OJK). However, in the community there are also other types of institutions that also carry out activities to raise funds from the public in the form of savings or some kind of savings, for example by post offices, pension funds, or insurance companies. The activities of these institutions are not included as banking business activities based on the provisions of the Banking Law. The activities of raising funds from the public carried out by these institutions are regulated by a separate Law. The threat of punishment for criminal offenses related to licensing is regulated in Article 462 of the Banking Law, which reads: "(1) Any person who collects funds from the public in the form of deposits without a business license from the Management of Bank Indonesia as referred to in Article 16, shall be punished with imprisonment at the minimum. -a minimum of 5 (five) years and a maximum of 15 (fifteen) years and a fine of at least Rp. 10,000,000,000.00 (ten billion rupiah) and a maximum of Rp. 200,000,000,000.00 (two hundred billion rupiah). (2) In the event that the activities referred to in paragraph (1) are carried out by Article 46 of the Banking Law analogous to Article 59 of the Limited Sharia Banking Law, unions, foundations or cooperatives, then prosecution of these agencies shall be carried out against those who to give orders to do the action or to act as the leader in the act or to both". legal entity in the form of a company. The description of bank crime in Article 46 paragraph (1) of the Banking Law is:

1. Anyone who includes all parties, namely:

a. person, such as an individual, is a person who is capable of committing legal acts, but does not include people whose actions cannot be legally accounted for, for example people who act based on orders from their superiors.

b. bodies, can be in the form of legal entities, namely bodies established with the approval of the relevant government agencies to carry out certain activities, such as Limited Liability Companies (PT. Closed or PT. Open / go public), cooperatives, foundations, and unions based on the relevant laws and regulations set it up. Non-Legal Entity, namely an entity established in the framework of carrying out business activities whose establishment does not require the approval of government agencies, such as CVs, Firms, and Civil Associations and other Entities.

2. Raising funds from the public, "raising funds" is an active act carried out by the perpetrator so that the public will hand over their funds to those concerned to be saved as demand deposits, deposits, certificates of deposit, savings, or other equivalent forms. Meanwhile, "community" includes individuals or legal entities or business entities or other parties who submit funds for safekeeping.

3. In the form of deposits, "deposits" are funds entrusted by the public to the bank based on a fund deposit agreement in the form of demand deposits, deposits, certificates of deposit, savings, and / or other equivalent forms. Deposits have properties and forms, including:

a. The characteristics of deposits in the form of demand deposits; there is a transfer of funds from the public, the withdrawal can be made at any time by means of a check, bilyet giro, other means of payment, or by book-entry, and can be given a reward in the form of money with a certain percentage.

b. The characteristics of deposits in the form of deposits; there is a handover of funds from the public, a receipt or proof of savings to the depositor, the withdrawal can be made at a certain time based on the agreement between the depositing customer and the bank, and there is a reward in the form of money with a certain percentage.

c. The characteristics of deposits in the form of certificates of deposit; there is a handover of funds from the public, a certificate of proof of deposit that can be physically transferred or recorded as proof of ownership (for scripless deposit types), the withdrawal can be made at a certain time based on the agreement between the depositing customer and the bank, and there is a reward in the form of money with a certain percentage.

d. The characteristics of savings are in the form of savings; there is a delivery of funds from the public, the withdrawal can be made according to certain agreed terms, but it cannot be withdrawn by check, bilyet giro, and / or other similar means, and there is a cash reward with a certain percentage. "Other equivalent forms" are intended to accommodate bank products that are not in the form of demand deposits, deposits, certificates of deposit, savings, but which have characteristics comparable to current accounts, time deposits, certificates of deposit, or savings.

4. Without a business license from the Management of Bank Indonesia (currently the Chairman of the OJK), this element confirms that only certain parties who have obtained a business license as a bank (Commercial Bank or Rural Bank) from the Management of Bank Indonesia (currently the Chairman of the OJK) can carry out activities of collecting funds, unless the activities of raising funds from the community concerned are regulated by a separate Law, for example the Post Office, Pension Fund, or Insurance Company.

The application of Article 46 paragraph (1) of the Banking Law is that individuals or Limited Liability Companies, Cooperatives, Foundations, Associations, CVs, Firms, or other entities are subject to criminal sanctions if they do not obtain permission from Bank Indonesia (currently OJK) in the event of doing so. collecting funds from the public or carrying out activities such as Commercial Banks or Rural Banks. The imposition of cumulative criminal sanctions in the form of imprisonment for 5 s.d. 15 years and a fine of Rp.10,000,000,000.00 up to Rp. Rp. 200,000,000,000.00.

Elucidation on tipibank in Article 46 paragraph (2) of the Banking Law is the issuer of orders and / or parties acting as the leader of a legal entity in the form of a Limited Liability Company, Union, Foundation or Cooperative, to raise funds from the public, in the form of savings, and without a business license from the Management of Bank Indonesia (currently the Chairman of the OJK) as a Commercial Bank or Rural Bank. This means that if the activity of collecting funds is carried out by a legal entity of a Limited Liability Company, Union, Foundation, or Cooperative, then the party responsible or who can be prosecuted is the person who gives the order to raise funds, or the party acting as the leader or leader in collecting funds, or both. . Meanwhile, for non-legal business entities or other entities, the legal responsibility of these business entities can be borne by individuals who are directly involved in the management of the agency as regulated in the Indonesian Commercial Code, Civil Code, and / or other related regulations. The application of Article 46 paragraph (2) of the Banking Law is if the fundraising activity is carried out by a certain form of legal entity such as a Limited Liability Company: shareholders, directors, commissioners, or employees; association: individual or administrator;

Cooperative: the founder, supervisor, supervisor, manager or member; or Foundation: the party that gives orders and / or leads the collection of funds, can be criminally charged with being accountable for their actions, with a cumulative criminal sanction in the form of imprisonment: 5 to 15 years and a fine: Rp.10,000,000,000.00 up to Rp. Rp. 200,000,000,000.00.

B. Banking Crime Relating to Bank Secrecy

The scope of bank secrets includes information about depositing customers and their deposits. Banks as an intermediary institution in carrying out their business activities always rely on elements of public trust, especially the trust of depositors who place their deposits in the bank. Banks as a trust institution are obliged to keep everything related to information regarding depositing customers and customer deposits at the bank confidential. The relationship between a bank and its customers is not like an ordinary contractual relationship, however, in this relationship there is also an obligation for the bank not to disclose the secrets of its customers to any party, unless otherwise stipulated by the prevailing laws and regulations. The common practice that banks must keep confidential is all data and information regarding everything related to finance and other matters of persons and entities known to the bank due to its business activities. Bank secrets are needed as a factor in maintaining the trust of depositing customers. Exceptions to the bank secrecy provisions include:

1. For tax purposes, upon a written order from the Management of Bank Indonesia (currently the Chairman of the OJK);
2. For settlement of bank receivables that have been submitted to BUPLN / PUPN, with the permission of the Management of Bank Indonesia (currently the Chairman of the OJK);
3. For the purposes of criminal court proceedings, with the permission of the Management of Bank Indonesia (currently the Chairman of the OJK);
4. In a civil case between a bank and its customer, for information from the bank's board of directors to the court regarding the financial condition of the customer;
5. In the context of exchanging information between banks, for information from the bank's board of directors to other banks regarding the financial condition of their customers;
6. At the request, approval, or power of attorney of the depositing customer in writing; and
7. At the request of a legal heir of a depositing customer who has passed away.

Opening of bank secrets as referred to in items 1 to 3 requires prior written permission to disclose bank secrets from the Management of Bank Indonesia (currently the Chairman of the OJK). Meanwhile items 4) to 7) do not require permission to disclose bank secrets from the Head of Bank Indonesia (currently the Chairman of the OJK). Criminal provisions relating to bank secrecy are regulated in Article 47 which reads: "(1) Anyone without a written order or permission from the Management of Bank Indonesia as referred to in Article 41, Article 41A, and Article 42, deliberately forces the bank or Affiliated Party to provide information as referred to in Article 40, is punishable by imprisonment of at least 2 (two) years and a maximum of 4 (four) years and a fine of at least Rp.10,000,000,000.00 (ten billion rupiah) and a maximum of Rp.200,000 .000,000.00 (two hundred billion rupiah). (2) Members of the Board of Commissioners, Directors, bank employees or other Affiliated Parties who knowingly provide information which must be kept confidential under Article 40, shall be punished with imprisonment of at least 2 (two) years and a maximum of 4 (four) years and a fine of at least. -a minimum of IDR 4,000,000,000.00 (four billion rupiah) and a maximum of IDR 8,000,000,000.00 (eight billion rupiah) ", and Article 47A of the Banking Law which reads:" Members of the Board of Commissioners, Directors, or employees a bank that deliberately fails to provide information that must be fulfilled as referred to in Article 42A and Article 44A, shall be punished with imprisonment of at least 2 (two) years and a maximum of 7 (seven) years and a fine of at least Rp. 4,000,000,000. 00 (four billion rupiah) and a maximum of Rp. 15,000,000,000.00 (fifteen billion rupiah) ". Article 40 paragraph (1) of the Banking Law has been amended based on the Decision of the Constitutional Court No.64 / PUU-X / 2012 dated 27 July 2012, to become: "Banks are required to keep information regarding their depositing customers and their deposits confidential, except in the cases referred to in Article 41, Article 41A, Article 42, Article 43, Article 44, and Article 44A as well as for judicial interests regarding joint assets in divorce cases ". The consideration of the Constitutional Court (MK) is in the context of fulfilling a sense of justice, so that customer data must also be disclosed for the benefit of the civil court related to joint assets, because joint property is joint property of husband and wife, so husband / wife must receive protection of their rights may not be taken arbitrarily by either party.

This is guaranteed by Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution. The considerations of the Constitutional Court (MK) are aimed at protecting the rights of husbands and / or wives to

joint assets stored in banks; protection of bank secrecy, so that customers' trust in the bank is maintained; and the existence of guarantees and legal certainty for the wife / husband for information regarding joint assets in marriage that is kept in the bank. The explanation of fraud in Article 47 paragraph (1) of the Banking Law is: Whoever is the same as the description of the element "Whoever" above . Without carrying a written order or permission from the Management of Bank Indonesia as referred to in Article 41, Article 41A, and Article 42, namely: the party as referred to in number 1) above, does not carry a written order or permission to open bank secrets from the Management of Bank Indonesia (when this is the Chairman of the OJK) as stipulated in Article 41, Article 41A, and Article 42 of the Banking Law, to request data on depositing customers and their deposits. Written orders or permits from the Management of Bank Indonesia (currently the Chairman of OJK) are addressed to banks for the following matters:

a. For tax purposes, a written order contains: the name of the tax official and the name of the taxpayer's customer for which information is desired.

b. For settlement of bank receivables, written permission shall contain: the name and position of the State Accounts Receivable and Auction Affairs Agency / State Receivables Affairs Committee, the name of the Debtor Customer, and the reason for the need for information.

c. In the interests of the judiciary in criminal cases, written permission shall contain: names and positions of the police, prosecutors or judges; the name of the suspect or defendant, the reasons for the need for information, and the relationship of the criminal case concerned with the information required.

The procedure for opening special bank secrets for the purposes of criminal court proceedings is regulated in Article 42 of the Banking Law which reads:

1. For judicial purposes in criminal cases, the Management of Bank Indonesia may grant permission to the police, prosecutors or judges to obtain information from the bank regarding deposits of suspects or defendants in the bank.

2. The permit as referred to in paragraph (1) shall be granted in writing upon a written request from the Chief of the Police of the Republic of Indonesia, the Attorney General, or the Chief Justice of the Supreme Court.

3. The request as meant in paragraph (2) must state the name and position of the police, prosecutor or judge, name of the suspect or defendant, the reasons for the need for information and the relationship of the criminal case concerned with the information required". If the request for disclosure of bank secrets has met the requirements, then no later than 14 days after receipt of the complete request documents, the Head of Bank Indonesia (currently the Head of OJK) will grant permission to disclose bank secrets. Requirements and procedures for issuing written orders or permits to disclose bank secrets must state:

a. ame and position of police, prosecutor or judge;

b. the name of the suspect or defendant;

c. name of the bank office where the suspect or defendant has deposits;

d. information requested;

e. the reason for the need for information; and

f. the relationship of the criminal case concerned with the information required.

This is intended so that requests for permission to obtain information from banks on a criminal case which is processed at all levels outside the general court are carried out in coordination between agencies, the implementation of which refers to the prevailing laws and regulations. Based on the permit for disclosure of bank secrets from the Management of Bank Indonesia (currently the Chairman of the OJK), the bank is required to carry out the order or license by providing information both orally and in writing, showing written evidence, letters, and printed electronic data, regarding the situation the financial services of the depositing customer as stated in the written permission. If the request letter does not meet the requirements according to the provisions, the Governor of Bank Indonesia (currently the Chairman of the OJK Board of Commissioners) may refuse to grant permission to disclose bank secrets. Refusal to grant permission to disclose bank secrets is notified in writing no later than 14 (fourteen) days after receipt of the request letter. 3) Intentionally, it can be seen, among others, based on the following matters:

a. there are regulations regarding this matter, both internal and external;

b. these regulations are violated / not implemented properly;

c. the perpetrator does his actions consciously; or

d. the perpetrator has the intention / intention in carrying out the action, whether it is pre-planned or not.

4. Forcing a bank or an Affiliated Party, the element of "forcing" has criteria including: threats accompanied by physical violence, pressure, intimidation, intimidation, or other forms of coercion against the bank or Affiliated Party, so that the bank or the Affiliated Party cannot act. other than providing the information requested. The element of "forcing" must be read in its entirety, namely "... forcing ... to provide confidential information". Meanwhile, the parties that force it are other parties, while the parties that are forced are banks and Affiliated Parties. In this connection, coercion is carried out in order for the bank and its Affiliated Parties to provide the requested information. That is, the "force" element stands alone and does not need to be followed by the achievement of the expected goals. Coercion is carried out on the bank or an Affiliated Party who is reasonably suspected of knowing the information requested by the perpetrator. The bank can include the bank as a legal entity, or an individual in the bank, namely a member of the board of commissioners, directors, or a bank employee. The term Affiliated Party is defined as:

a. members of the board of commissioners, supervisors, directors or their proxies, officers or employees of the bank;

b. members of the management, supervisors, managers or proxies, officers, or bank employees, especially for banks that are in the form of a cooperative law in accordance with the prevailing laws and regulations;

c. parties providing services to banks, including accountants in Article 1 number 22 of the Banking Law. other consultants; public, appraiser, legal consultant and

d. parties who according to the assessment of Bank Indonesia (currently OJK) participate in influencing bank management, including shareholders and their families, families of commissioners, families of supervisors, families of directors, families of managers. Providing information as referred to in Article 40. Coercion by the perpetrator is intended to cause the bank and / or Affiliated Parties to provide the information referred to in Article 40 of the Banking Law, namely information regarding Depositors and their deposits. Depositors4 are defined as customers who place their funds in a bank in the form of deposits pursuant to Article 1 number 17 of the relevant Banking Law. Information can include Personal Data of Depositors and any information related to deposits. Bank agreements with customers applying the provisions of Article 47 paragraph (1) of the Banking Law are parties who do not carry written orders or permits from Bank Indonesia (currently OJK) are subject to cumulative criminal sanctions, namely imprisonment of 2 to 4 years and criminal a fine of Rp. 10,000,000,000.00 to Rp. 200,000,000,000.00 if deliberately forcing the bank or bank affiliated parties, such as shareholders, directors, or commissioners including attorneys and their families, consultants, and other affiliated parties, to provide information concerning customers of the bank concerned and their deposits, for example the name of the customer and the amount of deposits, in relation to taxation purposes, settlement of bank receivables that have been submitted to the State Receivables and Auction Agency and the interest in settlement of cases in court. Elucidation on tipibank in Article 47 paragraph (2) of the Banking Law is: First. members of the Board of Commissioners, Directors, bank employees, or other Affiliated Parties, are parties appointed as commissioners, directors, or employees in accordance with the provisions applicable to the bank concerned (both permanent and honorary employees, including outsourcing in accordance with applicable manpower regulations), actively served as commissioners, directors, and / or bank employees at the time the crime was committed.

Meanwhile, Affiliated Parties are parties as described in Article 1 number 22 of the Banking Law. Intentionally, is the same as the description of the "Intentionally" element above. Second, to provide information which must be kept confidential according to Article 40, which is entered into with information is information regarding the Deposit Customer and his deposits. Information can include Personal Data of Depositors and any information related to deposits. The application of the provisions of Article 47 paragraph (2) of the Banking Law, members of the board of commissioners or directors, bank employees including their attorneys and their families, shareholders, consultants, and other affiliated parties are subject to cumulative criminal sanctions, namely imprisonment 2 to 4. years and a fine of Rp. 4,000,000,000.00 to Rp. 8,000,000,000.00, if deliberately providing information about the customer and the bank's savings, for example the name and amount of deposits. The explanation of tipibank in Article 47A of the Banking Law is: Members of the Board of Commissioners, Directors, or bank employees, are the same as the description of the element “Members of the Board of Commissioners, Directors, or bank employees” above. Intentionally, is the same as the description of the "Intentionally" element above. Failure to provide information that must be fulfilled as referred to in Article 42A and Article 44A, Information is information regarding customer deposits as requested by tax officers, BUPLN / PUPN officials, police, prosecutors, judges or depositors. For tax purposes, for settlement of bank receivables that have been submitted to BUPLN / PUPN, for judicial purposes in criminal cases, upon request, approval or power of attorney from the Deposit Customer made in writing, constitutes a condition for granting permission to disclose bank secrets. With the application of the provisions of Article 47A of the Banking Law, members of the board of

commissioners, directors, or bank employees are subject to cumulative criminal sanctions, namely imprisonment of 2 to 7 years and a fine of Rp. 4,000,000,000.00 to Rp. 15,000,000,000.00 if intentionally failing to provide information about customer deposits as requested by related parties for tax purposes, settlement of bank receivables, judicial interests in criminal cases, or at the request of the customer concerned. Based on the description, it can be concluded that the parties subject to criminal threats in relation to the provisions on bank secrecy are:

1. A party deliberately forcing a bank to provide information which must be kept confidential.

2. Directors, commissioners, bank employees who deliberately disclose information that must be kept confidential.

3. Directors, commissioners, bank employees who deliberately fail to provide information that must be fulfilled.

The provisions on bank secrecy are so strict and the imposition of severe criminal sanctions for those who violate them, giving the impression that the banking world is hiding behind bank secrecy provisions to protect the interests of customers which are not necessarily true, but if the bank really protects the interests of its honest and clean customers, then this is a necessity and propriety.

C. Bank Breaking Cases in Indonesia

Bank crime (tipibank) in Indonesia is not a new thing in this country, because in fact there are indeed many cases of banking crimes with various modes of crime committed by unscrupulous bank employees themselves. Complaints from bank customers from various banks emerged, from small and large scale losses. This banking crime can be said to be an extraordinary crime, because most of the perpetrators of bank crimes are committed by intellectuals who are highly educated. This bank crime is carried out in a very systematic, neat and structured manner by enabling internal bank officials and third parties who control and understand the digital technology applications of these banks. This bank crime occurs because there are several factors that become the main cause, namely deviations in moral behavior in addition to other factors. In its true inner self and the depth and sharpness of analysis as well as clarity of thought and perspective in conceptualizing the flow of human thought, it resides in the heart and heart. Whether he will commit transgressions or crimes, it is the human heart that makes him evil and good according to the will of his heart. This means that banking criminal acts occur not only because of the outward factor of factually violating the law, but also internally there have been problems in structuring morality and ethics in carrying out their main duties. Morality is in touch with the teachings of religious dogma and theology which are good for structuring the heart and heart of the perpetrators of banking crime. By fostering good morality and ethics, it will also minimize banking crime in Indonesia. A legal scientific philosophical approach and a religious approach in an effort to enforce and reformulate criminal law in Indonesia are necessary and must be mandatory. A religious approach in law enforcement efforts must color the rhythm of the implementation and execution of the law that has been carried out by law enforcement officials. Not only imposing criminal sanctions, but on the other hand, prevention of criminal acts using a religious approach is also required by means of outreach to the public as well as to officials and employees of banks in Indonesia.

The case of the loss of customer savings at Bank Maybank Indonesia occurred some time ago. Fortunately, customers who lost their savings at Maybank Indonesia, named Winda Earl, will receive replacement money. PT Bank Maybank Indonesia Tbk is finally committed to replacing money for e-sports athlete Winda Earl. However, the money that was replaced was not a total of Rp. 22.9 billion, but only Rp. 16.8 billion. "We have stated our readiness to replace Rp. 16.8 billion," said PT Bank Maybank Indonesia Tbk spokesman Tommy Hersyaputera to Kompas.com, Wednesday (11/25/2020). Tommy said that the commitment for replacement money came from a mediation process facilitated by the Consumer Protection Department, the Financial Services Authority (OJK). As for now, the mediation process is still continuing. The remaining money that has not been reimbursed will await the investigation process from the National Police Headquarters. "While the rest are still waiting for the investigation process by friends in the police. Furthermore, he asked for cooperation from all parties to jointly respect the ongoing investigation. Through the investigation, he hopes that all parties who receive funds in this case will be clearly revealed. .

Furthermore, the case of lost money from savings also occurred in one of the BRI customers. Warganet is again enlivened by the sudden loss of bank customer balances. This time, the incident happened to a customer of PT Bank Rakyat Indonesia (Persero) Tbk. The customer told what happened to him via Twitter. Through the @abunga *** account, the customer said that he had lost a total of Rp. 16 million on December 25, 2019. “Right when I woke up at dawn prayers and switched on my cellphone, suddenly I received a withdrawal notification several times totaling 16 million. The customer then immediately contacts BRI to make a report and block the ATM card. He also went to the nearest BRI office to report what had happened to him. However, when making the report, the customer received an explanation that it was impossible to withdraw money via ATM up to Rp. 16

million per day. BRI has informed that the maximum withdrawal of money through an ATM is IDR 10 million per day for the type of card used by the customer. He also received an SMS notification from BRI that the transaction that happened to him was in the normal category. "I have met with the BRI for further investigation and a settlement was promised this week. BRI Operations Director Indra Utoyo said, if a customer reports that their funds are reduced, but the customer feels that they are not taking their own funds, his party will investigate first. The bank will immediately follow up by carrying out a complete investigation including the possibility of whether the withdrawal is normal using the customer's ATM card or there are indications of fraud skimming. He added that the company will always upgrade its security system for e-banking transactions, "so that customers don't have to worry."

Bank burglary cases also occurred involving company leaders, namely, the director of PT Banyumas Citra Televisi (Banyumas TV), Firdaus Vidhyawan, accused of breaking into the Purbalingga branch of Bank Rakyat Indonesia up to Rp 28.7 billion. The credit break-in mode uses the name of a person who is recognized as an employee of the company. In a trial at the Corruption Eradication Court in Semarang, Firdaus was charged together with CV Cahaya Aang Eka Nugraha's director and the company's flag, which is still in the same corporate group, Yeni Irawati. Public prosecutor Sri Heryono said the crime itself occurred between 2015 and 2017. The defendants were known to have applied for credit to the Purbalingga Branch of Bank Rakyat Indonesia by handling the funerals of employees whose wages were paid by pay roll at a state bank. During that period, the defendants had submitted 171 names to obtain loans approved and disbursed by Bank Rakyat Indonesia. It was later discovered that the 89 people and 171 names of the debtors were not permanent employees at the company headed by the defendants. The 89 debtors are identified as people whose names have only been borrowed and are recognized as permanent employees. After the BRIGuna credit was approved and disbursed, he said, only 3 percent was given to the debtor, while the defendant took the rest in cash. For their actions, the defendants were charged under Article 2 Paragraph 1 or Article 3 of Law Number 31 of 1999 which has been amended by Law Number 20 of 2001 concerning the eradication of corruption. Apart from the three defendants, there were also two BRI employees of the Purbalingga branch who were tried in separate files in the same case. The two employees of Bank Rakyat Indonesia are Associate Account Officer of BRI Purbalingga Imam Sidrajat and Account Officer Endah Setiorini. Both were charged with being involved in the burglary because they agreed to apply for the loans of the 171 problem debtors. The two defendants agreed to and disbursed the loan without going through the correct survey of the prospective borrower.

Bank burglary cases also occurred in Central Java Bank. The defendant broke into cash amounting to Rp 4.4 billion belonging to the Pekalongan Branch of the Central Java Bank. M. Fredian Husni, the defendant, was found to have committed this crime for 1 year without being even once suspected by the management of a regional owned company (BUMD) in Central Java Province. Fredian when examined as a defendant in a trial at the Semarang Corruption Court, Tuesday, January 8, 2019, was a contract employee of Bank Jateng. He admitted that he took money during the ATM filling process from May 2017 to May 2018. During that period, the defendant was never reprimanded or warned once, even though there were irregularities in the financial statements. The stolen money, he continued, was entirely used to play online gambling. All for gambling, nothing is used to buy things or give to other people. Fredian revealed a number of ways he did to take the bank's money. One of the ways this is done, he said, is by taking the money directly after the transaction process of withdrawing from the big treasury of Bank Jateng. So, for example, I took Rp. 200 million, after that I immediately took Rp. 100 million. Then the rest goes to the ATM machine. After inserting the money into the ATM, the defendant then tricked the report documents that had to be returned to the big cashier. He also admitted that he tricked his companion in the process of replenishing ATMs into not realizing that the nominal reported was actually not correct. Regarding the procedure for transporting money from the office to the ATM machine, the defendant admitted that the process of carrying money worth hundreds of millions of rupiah used a plastic bag instead of a money storage box. According to him, apart from the limited storage box for money, the technicality of transporting money using a plastic bag has been taught since training for prospective employees.

Strategic Indonesia noted that in the first quarter of 2011, there were nine bank fraud cases in various banking industries. Jos Luhukay, an observer of Indonesia's Strategic Banking, said that the mode of banking crime is not only a matter of fraud, but the weakness of the bank's internal control over human resources is also an opening point for banking crimes. Internal control is a major banking problem. Bank Indonesia must set a standard operating procedure (SOP). The following are nine banking cases in the first quarter compiled by Strategic Indonesia through the National Police Headquarters Criminal Investigation Agency:

1. Bank Rakyat Indonesia (BRI) Tamini Square Cash Office burglary. Involving the cash office supervisor was assisted by four suspects from outside the bank. The mode is to open an account in the suspect's name outside the bank. Money transferred to this account amounted to 6 million US dollars. Then the money was exchanged for black dollars (fake US dollars in black) to become 60 million US dollars.

2. Providing credit with fictitious documents and guarantees to Bank Internasional Indonesia (BII) on January 31, 2011. Involving the BII Pangeran Jayakarta branch account. The total loss was Rp. 3.6 billion.
3. Withdrawal of deposits and escape theft of Bank Mandiri customer savings. Involving five suspects, one of which is the bank's customer service. His mode of action is to fake the signature on the withdrawal slip, then transfer it to the suspect's account. Case reported on February 1, 2011, with a loss value of Rp 18 billion.
4. Bank Negara Indonesia (BNI) Margonda Depok Branch. The suspect is a representative of the BNI branch leadership. The method is, the suspect sends fake telex news containing an order to remove the credit decree slip by opening a working capital loan account.
5. Disbursement of deposits of Rp 6 billion belonging to customers by BPR managers without the knowledge of the owners at BPR Pundi Artha Sejahtera, Bekasi, West Java. At the maturity date of the deposit there is no fund This case involved the Managing Director of the BPR, two commissioners, the main commissioner, and a perpetrator from outside the bank.
6. On March 9th happened to Bank Danamon. The method used by the head teller at Bank Danamon's Menara Bank Danamon branch was to withdraw cash from customers repeatedly amounting to Rp 1.9 billion and US $ 110,000.
7. Embezzlement of customer funds by the Head of Operations at Panin Bank, Metro Sunter Branch, by channeling funds to personal accounts. Bank losses of Rp 2.5 billion.
8. The burglary of Citibank Landmark priority customer money worth Rp. 16.63 billion was carried out by the bank's senior relationship manager (RM). Inong Malinda Dee, as RM, withdrew customer funds without the owner's knowledge through a blank withdrawal slip that had been signed by the customer.
9. Conspiracy of fraudulent investment / deposits worth Rp. 111 billion for the personal benefit of the Head of the Bank Mega Jababeka Branch and the Finance Director of PT Elnusa Tbk.

Looking at the various cases of banking crime in Indonesia and to maintain and provide legal protection for customers, the government really must carry out strict supervision and especially from the Financial Services Authority (OJK), Bank Indonesia (BI), and both bank supervisory institutions internal or external.

D. Customer Must Understand Technology

From the explanation of the results of the discussion above, it is found empirical facts that there are many modes of banking crime. The perpetrators come from internal officials at the bank itself with various modes of stealing customer money through manipulation of financial reports, falsifying customer data, and manipulating the banking system by digitizing illegal transfers of funds. Advances in information technology as well as advances in telecommunications technology have changed many things, from the way people live, how to work, and how to communicate. So that it is necessary to adjust technology to the public so that they do not miss information and technology, so as to prevent the occurrence of banking Cyber Crime crime and to save deposit funds in banks in Indonesia. The law should make people happy, because if the law cannot be enforced, it will make people sick and unhappy. Do not let the law dry up because the law loses its purpose. This also underlies the emergence of fundamental changes in banking technology, from a bank with an old concept (paper based) to a modern bank with digital services. Then a new concept emerged, banking services with the principle of anytime - anywhere banking. A banking service that enables interactions between customers and banks to be carried out any time, anytime and anywhere. This service is a banking effort to overcome the limitations of using ATM cards which are limited from the physical aspect of their use. In general, there are 3 digital banking services, namely: SMS Banking, m-Banking (mobile banking) and internet banking. Internet banking is the simplest digital banking service, where the main platform is an internet connection. This service can be enjoyed by customers using a desktop computer or smartphone. The key is in an account that is verified by the bank as an account that is directly correlated with the customer's personal data. Meanwhile, for SMS Banking and m-Banking, apart from verification of customer data, the important thing to be able to run this service is verification of the customer's cellphone number and SIM card data. In this case, the cellphone number and SIM Card must be registered with the bank so that the customer can run SMS Banking or m-Banking services. Seeing the ease of service in carrying out banking transactions, m-banking tends to increase its users compared to SMS banking.

Furthermore, for internet banking, the type of banking crime that is generally committed is the theft of customer's username and password. Phishing techniques through the ASPAL web (real but fake) from banking services are often used as the first step to carry out this type of crime in internet banking. The customer must be careful when opening a bank site that is a provider of banking services. Criminals will create a site that is similar to the official website both in terms of address and appearance. If the customer is deceived by this asphalt web, then with the username and password entered into the asphalt web, the perpetrator of the crime will take the next steps to use the username and password for his own benefit. This includes conducting banking transactions without the knowledge of the owner of the customer. For SMS Banking and m-banking, the type of crime committed is to carry out SIM Card Swaps, which is an attempt to trick cellular operators into requesting a SIM card change from a certain number. This technique is used to be able to take over a cellphone number with the

target of accessing the banking account registered on that mobile number. In this case, the perpetrator must first convince the service provider that his application to change the SIM Card is valid and can be approved. The procedure for changing the SIM card itself is actually very strict, although each service provider has different SOPs, they try to prevent the change of SIM cards by irresponsible people. Therefore, an indication of organized crime is a very reasonable conclusion if it turns out that the process of changing SIM cards by irresponsible people can be done easily and quickly. The perpetrator of this SIM Card Swap crime knows well the potential victim as well as the latest position and track record of banking transactions of the potential victim. It is impossible for the perpetrator to carry out a SIM Card Swap on a potential victim who does not have a track record of the potential victim's customers. One indication that there has been a SIM Card Swap attempt on our cellular number is if it suddenly turns out that the cellphone number and SIM Card suddenly cannot be actively used. The reasonable guess from the SIM card owner is that there is damage to the SIM card or there is a network problem so that the cellphone number cannot be used. Therefore, if the SIM Card on our cellphone suddenly cannot be used, we must immediately contact our service provider. Another thing that is also the procedure for replacing the SIM Card is having to turn off the cellphone where the old SIM Card is installed. So if suddenly you get a call / SMS on behalf of a cellular operator asking us to temporarily turn off our cellphone under any pretext, it must be ignored and suspected as an attempt to take over the SIM Card. Apart from not being able to use the SIM Card, another identification that shows the possibility that a SIM Card Swap has occurred is a notification that there are our activities in other places outside of the habit with different devices. Many applications carry out the fraud monitoring process through the detection of locations and devices connected to certain mobile numbers. If there is a change, the application will notify you via email about the change.

Enabling two-factor authentication security (2FA, Two Factor Authentication) is the control of our banking accounts from illegal activities that are carried out beyond our control. Through this security concept, if there is a request to the system to make changes to something from the data on our account, it will confirm it by sending an OTP (One Time Password) password to us through other media under our control (generally confirmation via email and SMS). So if you suddenly receive an SMS / Email containing an OTP from our banking account, you must immediately suspect it as an attempt to take over the account. The concept of 2FA and OTP becomes invalid if it turns out that upaua SIM Card Swap has been made. Because of this, the SIM card replacement process is approved by the service provider, so the 2FA and OTP mechanisms will be transferred to the cellphone that is under the control of the criminal. In addition, all m-banking service providers provide a feature to send notifications via SMS and Email when a debit or credit transaction has occurred on the customer's bank account. Although this service generally charges SMS / Email sending costs to its customers, it is very important as part of controlling various financial transactions on our banking accounts. The main drawback of the 2FA concept is the OTP message via SMS. The OTP text message sent via SMS / email is seen as one of the weaknesses exploited by SIM Card Swap actors. Because of that, the SIM Card has been taken over, so all OTP mechanisms of the services connected to the SIM Card will automatically be taken over. Because of this, many system security analysts have begun to consider the use of OTP via SMS. Another alternative technology is the use of services from Google Authenticator, Microsoft Authenticator, and Authy as part of the 2FA mechanism. This technology does not perform the OTP transmission process via text or email, but requires physical access to the cellphone directly, so that as long as the cellphone does not change control physically, the OTP process will be directly controlled by the owner of the cellphone. Profiling through social media is one of the stages of banking crimes. The use of Social Engineering Attack is one of the mechanisms. The availability of data is easily obtained through social media such as: email, ID number, cellphone number, name of family member, daily activities, last position, type of goods purchased, the store where we shop; are data that can be obtained by the perpetrator to determine whether a person is a target of SIM Card Swap.

4. Conclusion

To take preventive measures in the future, from being a victim of various banking crimes, differentiating data on social media accounts from banking data is a wise choice. Having a mobile number and special email for banking transactions is a safe choice for today's society. It is uncomfortable, but it will narrow the gap for certain parties who try to do profiling through the availability of personal data that is spread through social media. Therefore, to the public, it is advisable not to be too open about their personal data to the public, especially social media; because according to the facts, these data are often used by banking criminals to commit crimes. We must always be careful in social media, and also always be aware of cyber-crime.

References

Barda Nawawi Arief, Kebiajkan Formulasi Ketentuan Pidana Dalam Peraturan- Perundang-Undangan, Pustaka Magister Semarang, 2012.

Yopie Morna Immanuel Patiro, Antara Perintah Jabatan dan Kejahatan Jabatan Pegawai Negeri Sipil, Keni Media, 2013. Hlm 76

Hammersley, Martyn. (2019). From Positivism to Post-Positivism: Progress or Digression? Teoria Polityki. 3. 175-188. 10.4467/25440845TP.19.009.10292.

Edi Ribut Harwanto, Distortion Between Dogma And Democracy System in Enformcing Criminal Law Sanctions to Build Morality National Millenial Era Leader Until The And of Time And Civilozation of Secularism, Sai Wawai Publishing, Metro, 2020, hlm VIII

Edi Ribut Harwanto, Filosofi Pendekatan Keimuan Hukum Dengan Pendekatan nreligius Dalam Upaya Memaksimalkan dan Mereformasi Pelaksanaan Penegakan Hukum Pidana di Indonesia., Metro, 2021, hlm, XV

Satjipto Rajardjo, Penegakkan Hukum Progresif, Kompas Penerbit Buku, 2010, hlm 39

https://www.google.com/search?client=firefox-b d&q=KEJAHATAN+PERBANKAN+OLEH+BANK

https://keuangan.kontan.co.id/news/maybank-akan-ganti-uang-nasabah-winda-earl-yang-hilang-tapi-hanya-segini

https://bisnis.tempo.co/read/1297839/viral-dana-nasabah-bri-raib-dalam-semalam/full&view=ok

https://bisnis.tempo.co/read/1257674/direktur-tv-didakwa-bobol-bri-rp-287-miliar-begini-modusnya/full&view=ok

https://money.kompas.com/read/2011/05/03/09441743/Inilah.9.Kasus.Kejahatan.Perbankan.

https://fit.uii.ac.id/blog/2020/01/25/modus-dan-antisipasi-kejahatan-perbankan/

WWW.OJK.GO.ID