TABELLIUS Journal of Law
ISSN 2988-6201
published by Master of Notarial Law Faculty of Law Universitas Islam Sultan Agung Semarang

Implementation of Notary Marking at State-Owned Commercial Banks as High Risk Customers in the Context of Preventing and Eradicating Money Laundering Crimes

Andini Dyahlistia Permatarani[1)] & R. Sugiharto[2)]

[1)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA), Indonesia, E-mail: andini.dyahlistia@gmail.com

[2)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA), Indonesia, E-mail: sugiharto@unissula.ac.id

Abstract. *This study aims to determine and analyze the mechanisms and legal consequences of the implementation of notary marking at state-owned banks as high-risk customers in the context of preventing and eradicating money laundering crimes. The approach method in this research is sociological juridical. The research specification is analytical descriptive research. The data required includes field study data (field research) taken using the interview method and library research data. The data analysis method uses qualitative data analysis. Based on the research, it was concluded that the mechanism for marking notaries at BUMN Banks as high-risk customers is carried out in 3 (three) stages, namely customer on-boarding, on-going monitoring and post monitoring.*

Keywords: *Bank; Customer; Laundering; Money.*

1. Introduction

Technological advances, especially telecommunications and transportation, have enabled the mobility and dissemination of information in a very wide and fast range as if it were not influenced by geographical boundaries. Moreover, after the technological convergence between computers, electronics, telecommunications and broadcasting, it is as if national geographic boundaries

do not exist for the dissemination of information.[1] The world seems to be united in a big village, where relationships between humans are no longer limited to space and place, so that what is called a borderless world emerges. This change towards a global culture has strong implications for almost all aspects of life. In line with these conditions, international crimes that penetrate jurisdictional boundaries are also increasing in intensity. Therefore, it is necessary to be aware of crimes that have strong relevance to the use of communications technology and have an international dimension, namely money laundering.

The opportunity for Indonesia to become one of the countries targeted for money laundering originating from crime is quite open. This is because in Indonesia there are potential factors that are attractive to money laundering perpetrators, namely the combination of weaknesses in the social system and legal loopholes in the financial system, including a free foreign exchange system, the origin of the money invested and the development of the capital market, foreign exchange traders and banking networks that have expanded abroad.[2]

In general, money launderers try to hide or disguise the origin of assets resulting from criminal acts in various ways so that the assets resulting from criminal acts are difficult for law enforcement officials to trace so that they can freely use these assets for both legitimate and illegal activities. Therefore, the crime of money laundering (hereinafter referred to as TPPU) not only threatens the stability and integrity of the economic system and financial system, but can also endanger the foundations of social, national and state life based on Pancasila and the Constitution of the Republic of Indonesia. 1945.[3]

In order to combat the crime of money laundering and provide a strong legal basis to ensure certainty and effectiveness of law enforcement, the handling of TPPU in Indonesia is regulated in Law of the Republic of Indonesia Number 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering (hereinafter referred to as the PPTPPU Law) .

[1]M Dimyati Hartono, Five Steps to Building Good Government, (Jakarta: Ind Hill Co, 1997), p. 53.

[2]Sri Endah Wahyuningsih and Rismanto, Criminal Law Enforcement Policy for Combating Money Laundering in the Context of Criminal Law Reform in Indonesia, Journal of Legal Reform, Vol. II, No. 1 January – April 2015, p. 48.https://jurnal.unissula.ac.id/index.php/PH/article/view/1414

[3]Explanation of Law of the Republic of Indonesia Number 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering.

As for the PPTPPU Law, there is the involvement of banks as financial service providers to carry out tracing of assets resulting from TPPU. Banks have an important role, especially in implementing the principle of knowing your customer and reporting certain transactions to the financial intelligence unit authority or in Indonesia known as the Financial Transaction Reports and Analysis Center (PPATK) as material for analysis and then submitted to investigators. The obligation to apply the principle of recognizing service users and reporting customer financial transactions is further regulated in the provisions of the Financial Services Authority (OJK) and the Financial Transaction Reports and Analysis Center (PPATK).

In accordance with Article 4 paragraph (1) of Financial Services Authority Regulation (POJK) Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector, financial service providers (including banks) are obliged to identify, assess and understand the risks of criminal acts of money laundering, criminal acts of financing terrorism and/or funding the proliferation of weapons of mass destruction against customers; country or geographic area; products, services, transactions or distribution networks. One of the applications of a risk-based approach carried out by banks is identifying and assessing customer risks. This risk assessment is also applied to prospective customers who will enter into business relations with the bank.

Customers and/or potential customers are assessed at least at 3 (three) levels, namely low, medium and high risk customers. High risk customers are customers who, based on their background, identity, history and/or the results of risk assessments carried out by financial service providers, have a high risk of carrying out activities related to money laundering, terrorism financing and/or weapons proliferation funding.[4] In determining the assessment of high risk customers, banks are guided by the Regulation of the Head of the Center for Financial Transaction Reporting and Analysis (PerKa PPATK) Number: PER-02/1.02/PPATK/02/2015 dated 3 February 2015 concerning Categories of Service Users Who Have the Potential to Commit Money Laundering Crimes . As for

[4]Article 1 number 15 of the Republic of Indonesia Financial Services Authority Regulation Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.

Article 5 letter g of the PPATK Regulation, it is stated that one category of service users who have a high risk of potentially committing money laundering crimes are customers who have a certain profile, including advocates, curators, notaries, land deed officials, accountants, public accountants. , financial planner, or tax consultant, including employees who work in these professional offices.

The inclusion of the notary profession as one of the profiles of bank service users who have the potential to commit TPPU in the PPATK Perka above, of course raises polemics and question marks as to why it is so urgent that notaries are marked as high-risk customers when carrying out business relationships with banks. On the one hand, the notary himself has applied the Principle of Recognizing Service Users (PMPJ) to his clients and has become the reporting party for suspicious financial transactions so that he has minimized the existence of clients who have the potential to launder money using the notary's expert services. Therefore, all activities related to financial transactions carried out by notaries (or notary employees) through banks should not be related to money laundering transactions carried out by their clients.

However, high risk assessments for customers who are notaries are absolutely carried out by banks in Indonesia. One of the risk assessment practices carried out by State-Owned Commercial Banks is that banks will specifically mark customers with a job profile as a notary, including notary employees, as high-risk customers. Providing this mark will cause several implications that will be received by the notary and his employees when opening an account or financial transaction because the bank will implement strict customer due diligence related to the implementation of the Anti-Money Laundering (APU) and Funding Prevention programs. Terrorism (PPT) and Prevention of Funding for the Proliferation of Weapons of Mass Destruction (PPPSPM) as regulated in the provisions of the OJK and PPATK.

In connection with the above, the researcher wants to know and analyze how State-Owned Commercial Banks carry out marking of notaries as high-risk customers as well as the legal consequences of implementing this notary marking at State-Owned Commercial Banks in the context of preventing and eradicating the Crime of Money Laundering (TPPU).

2. Research Methods

The research method used in this research uses sociological juridical methods. The research specifications used are analytical descriptive research. Types and sources of data use field study data taken using interview methods and secondary data from library research. The data analysis method used is qualitative data analysis.

3. Results and Discussion

3.1 Mechanism for Implementing Notary Marking at State-Owned Commercial Banks as High Risk Customers in the Context of Preventing and Eradicating the Crime of Money Laundering (TPPU)

Article 4 paragraph (1) POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector, requires banks to identify, assess and understand the risks of Money Laundering Crimes (TPPU) , Terrorism Financing Crimes (TPPT) and/or Funding for the Proliferation of Weapons of Mass Destruction (PPSPM) against customers, countries or geographic areas, products, services, transactions or distribution networks. The risk assessment is carried out by the bank using the methodrisk-based approach (Risk Based Approach) as referring to POJK provisions and the Financial Action Task Force's Guidance for A Risk Based Approach (RBA) – The Banking Sector October 2014.

According to FATF's Guidance, A RBA to Anti Money Laundering (AML)/Countering Financing Terrorism (CFT) means that countries, competent authorities and financial institutions are expected to identify, assess and understand the Money Laundering (ML)/Terrorism Financing risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively (RBA against AML/CFT means that countries, competent authorities and financial institutions are expected to be able to identify, assess and understand TPPU risks /TPPT they face and take measurable actions to be able to mitigate these risks effectively).[5]When conducting a TPPU/TPPT assessment, the state, competent authorities and financial

[5]Section I – The FATF's RBA to AML/CFT, Financial Action Task Force's Guidance for A Risk Based Approach (RBA) – The Banking Sector October 2014, p. 6.

institutions must analyze and understand how the TPPU/TPPT risks they identify affect them. Therefore, risk assessment provides a basis for implementing ML/TF prevention measures.[6]

Based on Section III – FATF's Guidance, The RBA to AML/CFT aims to support the development of prevention and mitigation measures that are commensurate to the ML/TF risks identified. In the case of banks, this applies to the way banks allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to determine and detect ML/TF, including, where relevant, at group level (RBA against APU /PPT aims to support the development of risk prevention and mitigation taken by banks commensurate with identified TPPU/TPPT risks). RBA is applied by banks to determine how the bank allocates its compliance resources, how the bank organizes internal controls and their structure.[7]

Customer risk assessment regarding vulnerability to TPPU will produce levels/levels of customer risk profile assessment into at least 3 (three) levels, namely low risk customers, medium risk customers and high risk customers. Each level of customer risk in question determines the treatment that the bank will apply to the customer in order to carry out the process of introducing/exploring the customer's profile (commonly known as the Know Your Customer (KYC) process).[8]Apart from that, customer risk profiles are also useful for banks to determine what level and type of monitoring the bank will apply to its customers, as well as supporting the bank's decision-making process to start, continue or end business relationships with customers.[9]

Referring to the level of customer risk, the KYC process is divided into 3 (three) treatments, namely as follows:

a. Customer Due Diligence (CDD)

[6]Ibid.
[7]Section III– The FATF's RBA to AML/CFT, Financial Action Task Force's Guidance for A Risk Based Approach (RBA) – The Banking Sector October 2014., p. 17.
[8]Indonesian Bankers Association (IBI) and Banking Compliance Directors Communication Forum (FKDKP), Culture Start From The Top: Building a Compliance Culture, (Jakarta: PT Gramedia Pustaka Utama, 2018), p. 146.
[9]Section III– The FATF's RBA to AML/CFT, Financial Action Task Force's Guidance for A Risk Based Approach (RBA) – The Banking Sector October 2014., Op. Cit., p. 19.

CDD is an activity in the form of identification, verification and monitoring carried out by banks to ensure transactions are in accordance with the profile, characteristics and/or transaction patterns of prospective customers, customers or Walk In Customers (WIC).[10]CDD is carried out on customers in normal circumstances or with a moderate risk profile.[11]CDD activities include identifying customers and their beneficial owners if any; verify customer identity based on information, data or documents that are reliable and still valid in accordance with provisions; and understand the goals and nature of customer business relationships when faced with higher risk situations.

b. Simple Customer Due Diligence (CDD).

Simple CDD can be applied by banks to potential customers or customers and/or transactions where the risk level of TPPU, TPPT, and/or PPSPM includes low risk criteria based on identification that has been carried out through adequate risk analysis.[12]

c. Strict Customer Testing/Enhanced Due Diligence (EDD)

EDD is a more in-depth CDD action carried out by banks on prospective customers, clients or Walk In Customers (WIC) who are at high risk including State Officials/Politically Exposed Persons (PEP) and/or in high risk areas.[13]EDD is carried out by requesting additional information about customers; carry out additional searches (for example looking for customer information in trusted mass media); create intelligence reports regarding the risk profile of customers or beneficial owners as well as suspected customer involvement in criminal activities; verify sources of funds/wealth that may be involved with criminal

[10]Article 1 number 12 POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.
[11]Indonesian Bankers Association (IBI) and Banking Compliance Directors Communication Forum (FKDKP), Op. Cit., p. 147.
[12]Article 45 paragraph (1) POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.
[13]Article 1 number 14 POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.

activity and seek additional information from customers regarding the purpose and nature of business relationships with the bank.[14]

Banks are required to have an adequate risk management system to determine Prospective Customers, Customers, WIC, or Beneficial Owners who fall under high risk criteria.[15]High risk criteria for prospective customers, customers, WIC, or beneficial owners, pay attention to the following factors:[16]

a. Background or profile of Prospective Customers, Customers, WIC, or Beneficial Owners;

b. High risk financial services sector products to be used as a means of TPPU, TPPT, and/or PPSPM;

c. Transactions with parties originating from High Risk Countries;

d. Transactions do not match profile;

e. Included in the PEP category;

f. Prospective Customers, Customers, WIC, or Beneficial Owners' business fields include high-risk businesses;

g. The country or territory of origin, domicile, or conduct of the Customer or WIC transaction is a High Risk Country; and/or

h. Transactions carried out by customers or WIC are suspected of being related to criminal acts in the financial services sector, TPPU, TPPT, and/or PPSPM.

If Prospective Customers, Customers, WIC, or Beneficial Owners meet the high risk criteria, the bank is obliged to carry out EDD.[17]Determining the risk level of Prospective Customers, Customers, WIC, or Beneficial Owners which include high

[14]Section III– The FATF's RBA to AML/CFT, Financial Action Task Force's Guidance for A Risk Based Approach (RBA) – The Banking Sector October 2014., Loc. Cit.
[15]Article 35 paragraph (1) POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.
[16]Article 35 paragraph (2) POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.
[17]Article 35 paragraph (3) POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.

risk criteria, is based on the risks to be taken and the risks that the Bank can tolerate.[18]

One of the mechanisms used by banks to facilitate EDD activities is by providing special marking for high-risk customers. High risk customer flagging (flagging high risk customer) is carried out by the bank on customer profiles as follows:[19]

a. State Administrators/Politically Exposed Persons (PEP)

b. Parties related to PEP

c. Officials, employees, officials, and everyone who works in the field of public services, especially in the fields of licensing, procurement and distribution of public goods and services, state or regional revenues;

d. Officers, employees, or any person who works for and on behalf of a financial services provider;

e. Persons or entities whose names are listed on the list of suspected terrorists and terrorist organizations issued by the government;

f. Persons or entities whose names are listed on the sanction list issued by international organizations; and/or

g. Certain professions include advocates, curators, Notary Public, Land Deed Official, accountant, public accountant, financial planner, or tax consultant, including employees who works in the professional office.

Recently, money laundering crimes have begun to utilize the services of Notaries to assist and disguise assets obtained from the proceeds of crime. The money laundering methods used by the perpetrators are by purchasing real estate / house property using the facilities of the Notary profession. Money launderers do not use their own names in carrying out transactions and own assets so that they are not easy to trace.[20]The honorable profession of notary who is tasked with serving the public in the field of civil law should not be used as a means of

[18]Article 35 paragraph (4) POJK Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.
[19]Article 5 Perka PPATK Number: PER-02/1.02/PPATK/02/15 concerning Categories of Service Users Who Have the Potential to Commit the Crime of Money Laundering.
[20]Yunus Husein, The Crime of Money Laundering in the Perspective of International Law, (Jakarta: Institute for International Legal Studies, Faculty of Law, University of Indonesia, 2004), p. 5.

money laundering by criminals. This tarnishes the notary profession and creates a negative stigma in the eyes of the public.

The development of this money laundering mode has increasedThe provisions of Article 5 letter g of Perka PPATK Number: PER-02/1.02/PPATK/02/15 concerning Categories of Service Users Who Have the Potential to Commit the Crime of Money Laundering, cause banks to carry out risk assessments and marking of customers with a job profile as Notaries and notary employees . Risk assessment and marking for customers who are Notaries is carried out as a risk mitigation effort taken by the bank regarding the potential use of the Bank as a means of money laundering. This is also done by State-Owned Commercial Banks, one of which is PT Bank Rakyat Indonesia (Persero), Tbk (known as BRI).

Bank with Indonesian government share ownership of 53.19%[21]This means identifying and assessing risks for customers with a work background as a notary and notary employees by providing a high risk customer flag attached to the employment data recorded in the customer's Customer Identification File (CIF).[22]Employment data is one of the factors that supports the calculation of the risk assessment of money laundering crimes at BRI. The mechanism for marking notaries at Bank BRI as individual customers who are at high risk of money laundering is carried out through the following stages:

a. Customer On-Boarding Stage

*Customer On-Boarding*is the initial process of identifying potential customers before customers use banking products and services.[23]At this initial stage, known as the account opening process, BRI will identify and mitigate the risks of potential customers before the person concerned can become a partner as a customer. Bank officers will dig up information and ask for documents and verify personal data, employment data and financial data of prospective customers. Prospective customers with a job profile as a Notary can be asked to include a Notary Appointment Decree to ensure the correctness of the customer's work. At this stage, information and data on prospective customers will be input into BRI's core banking system, then the system will screen customer data to ensure

[21]BRI Annual Report 2022 p. 9,https://bri.co.id/report, accessed 19 August 2023.
[22]Results of Interview with Mrs. Mila Mulyani, Team Leader of AML-CFT Analyst & Reporting, BRI Compliance Division on August 9 2023.
[23] https://complyadvantage.com/insights/how-to-prioritize-risk-during-customer-onboarding/, accessed 19 August 2023.

whether the customer in question has any indication of TPPU involvement. Furthermore, This process is continued to calculate and assess customer risk to produce a score that determines the potential customer's risk level for TPPU. The results of customer risk identification become documentation data that must be managed by BRI, and the results of these risks will not be communicated to customers.

Prospective customers with employment data as a notary are marked as high risk customers. However, the results of risk calculations do not always produce the notary customer's score/score as a high risk customer, it could be that the notary customer's score is in a medium risk position. This happens because during the risk assessment process, the system will also consider other risk determining factors such as the source of income used as a source of account funds, the purpose of opening the account, the account opening channel, the notary's domicile, the notary's nationality, the product chosen, the delivery channel and transaction information.

If the customer's risk category is at high risk of money laundering/terrorist financing/funding the proliferation of weapons of mass destruction, then the process of opening an account at BRI must be approved by an appointed senior official, including a worker with the position of head of the Special Branch Office/Head of Operations Special Branch Offices, Branch Office Leaders/Operational Managers/Assistant Operational Managers, Priority Banking Managers, Sub-Branch Leaders and BRI Unit Heads. The approval from the senior official will form the customer's CIF data and customer account number.

Senior officials have the right to refuse to approve a customer's account opening if:

1. The customer does not want to fulfill requests for information and supporting documents required by BRI;

2. The customer is known and/or reasonably suspected of using fake documents such as identity documents (KTP, SIM, Passport) and/or other documents, apparently not registered with the authorized agency or whose authenticity cannot be verified;

3. The customer submits information whose veracity is doubtful;

4. The customer is included in the List of Suspected Terrorists and Terrorist Organizations or the List of Funding for Proliferation and Weapons of Mass Destruction; and/or

5. Customers are unwilling to provide financial information to BRI for the purposes of identifying and reporting domestic and international tax compliance.

b. On-going Monitoring Stage

This stage is where existing customers are monitored and evaluated by looking at developments in customer data profiles, volume and frequency of customer transactions, portfolio and types of products & services chosen by customers, whether customer transaction habits and patterns are still in line with the APU, PPT and PPSPM programs implemented. by BRI. At this stage, customer risk calculations and assessments are carried out again so that it is possible for there to be changes/shifts in the customer's risk profile. For example: a customer who works as a notary, initially had a medium risk as a customer, but as time progressed it turned out that the person concerned was a suspect or accused of money laundering, so the customer's risk shifted to high risk. Several things that cause customers to re-calculate their risks include:

1. There are large or complex transactions without clear transaction objectives;

2. There are small and frequent transactions that accumulate into large transactions;

3. Unusual transaction patterns, such as cash deposit-withdrawal transactions of significant amounts;

4. Transaction activities with destination or origin from high risk countries or areas;

5. Suddenly there is a significant transaction on an account that has been dormant for a long time;

6. *Negative news*regarding customer profiles in relation to TPPU/TPPT/PPSPM;

7. There are transaction activities detected involving money laundering/terrorism financing/proliferation funding and weapons of mass destruction, etc.

BRI will take risk mitigation steps, including giving a high risk flag to the customer's CIF, reporting the customer to PPATK in the Suspicious Transaction Report, collecting the latest customer information and updating customer data, as well as making efforts to maintain relationships. with customers.

c. Post Monitoring Stage

After building relationships with customers, the Bank is obliged to monitor customer profiles and transactions, either periodically reviewing or triggered by certain events (triggered events).[24]Post Monitoring is the stage where the Bank will maintain or close business relationships with customers (close the customer's account by returning the remaining funds). BRI's Anti Money Laundering and Counter Terrorist Financing (AML/CFT) system provides alert warnings to the Operational Work Unit when it encounters customer transactions that do not match the customer's activities or habits which might trigger suspicious transactions.

When the transaction anomaly occurs, the customer due diligence process is carried out again, as well as the customer risk assessment being calculated again. If the results of the investigation show that the customer is truly positively detected as being involved in money laundering activities/terrorism financing/proliferation funding and weapons of mass destruction, then BRI will take the position to report the customer to PPATK in a Suspicious Transaction Report, terminating the business relationship with the customer (close the customer's account by returning the remaining funds), and enter the customer into the internal negative list (BRI's internal list containing negative information about customers). If in the future the customer wants to open an account again at BRI, then BRI has the right to refuse the customer's wishes.

To obtain the latest information regarding the profile of customers who are notaries, BRI collects information sourced from national news from credible media, both print and online media. From these news stories, there is sometimes news information about money laundering involving notaries where the notary has been named as a suspect or defendant in a money laundering case. Apart from that, BRI also subscribes to third parties who provide databases of names of

[24] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidance-for-_Effective-AML-CFT-Transaction-Monitoring-Controls.pdf, accessed 21 August 2023.

people who have a negative reputation related to money laundering. These data sources are included in BRI's core banking system and BRI's AML/CFT system, thereby facilitating the process of screening customer profiles and assessing customer risk.

The latest data from customers who are notaries are required by BRI in order to identify the customer's risks. If it turns out that a notary has retired and BRI is aware of this change, then the high risk marking of the customer can be removed and the customer's risk is shifted to medium risk so that BRI only needs to monitor the customer's transactions and profile once a year. It's different if a notary customer is always marked as high risk, then monitoring his transactions and profile is always a priority for BRI, at least once every 6 (six) months. This monitoring has implications for changes in customer data, reporting to PPATK in the form of a Suspicious Transaction Report (STR) if there are indications of money laundering,

All stages of the notary marking mechanism mentioned above have been regulated in BRI policies and procedures regarding the Anti-Money Laundering (APU), Prevention of Terrorism Financing (PPT) and Prevention of Funding for Proliferation and Weapons of Mass Destruction (PPPSPM) programs. The implementation is also supervised internally by senior officials in the BRI Operational Work Unit and supervised by the Branch and BRI Risk Management and Compliance Units and Compliance Officers in Regional Offices or Overseas Branches. Apart from that, the policies and procedures as well as the implementation of the APU, PPT and PPPSPM programs are also reviewed by audit, both from BRI's internal audit and external auditors to ensure whether they are still in line with the provisions of the regulator.

3.2 Legal Consequences of the Implementation of Notary Marking at State-Owned Commercial Banks as High Risk Customers in the Context of Preventing and Eradicating the Crime of Money Laundering (TPPU)

The implementation of notary marking at State-Owned Commercial Banks as high-risk customers in the context of preventing and eradicating money laundering criminal acts has legal consequences, namely that State-Owned Commercial Banks are required to carry out risk assessments and identification related to the implementation of the Anti-Money Laundering (APU) program on a regular basis for customers with work as a notary. Violation of the

implementation and risk identification obligations will result in the Bank being subject to administrative sanctions from the Financial Services Authority (OJK), including in the form of:

a. A written warning or warning accompanied by an order to take certain actions;

b. Fine;

c. Restrictions on certain business activities;

d. Decreased assessment of factors forming the value of health level;

e. Suspension of certain business activities; and/or

f. Prohibition as the main party.

The Financial Services Authority (OJK) can announce the imposition of the above administrative sanctions to the public. Announcement of the imposition of administrative sanctions to the public can be made, among other things, through the Financial Services Authority page/website. The imposition of these administrative sanctions does not eliminate the obligation of state-owned banks to continue to carry out their obligations to implement the Anti-Money Laundering (APU) Program.

The imposition of administrative sanctions in the form of fines by the Financial Services Authority (OJK) on state-owned banks, calculated with the following provisions:[25]

a. The maximum per year is IDR 5,000,000,000.00 (five billion rupiah) for individuals;[26]and/or

b. A maximum of 1% (one percent) of the previous year's total net profit with a maximum limit per year of IDR 100,000,000,000.00 (one hundred billion rupiah) for state-owned banks.

[25]Article 79 paragraph (1) POJK no. 8 of 2023 concerning Implementation of Anti-Money Laundering (APU) Programs, Prevention of Terrorism Financing (PPT) and Prevention of Funding for the Proliferation of Weapons of Mass Destruction (PPPSPM) in the Financial Services Sector.
[26]Explanation of Article 79 paragraph (1) letter a POJK No. 8 of 2023, "natural person" means the Directors, Board of Commissioners, and/or PJK employees, including senior officials who are 1 (one) level below the Directors and Board of Commissioners.

If a BUMN Bank is only one of the units/divisions in another PJK, then the net profit calculation as referred to above is the net profit of the other PJK.[27]The calculation of the imposition of fines by the OJK is suspended for PJKs that experienced losses in the previous year. In the event that the PJK has made a profit, the calculation of fines is determined based on the net profit received.[28]

4. Conclusion

From the discussion above, it can be concluded that the mechanism for marking notaries at State-Owned Commercial Banks as customers at high risk of money laundering is carried out through 3 (three) stages, namely the customer on boarding stage, the*on-going monitoring*and post monitoring stage. In these three stages, risk calculations are carried out to determine the risk level of customers who work as notaries. Customers with a high level of risk will be given a marking in the form of flagging high risk customers so that strict customer tests (enhanced due diligence) and more frequent transaction monitoring will be implemented. In addition, marking notaries as customers at high risk of money laundering has legal consequences, namely State-Owned Commercial Banksis obliged to carry out risk assessments and identification related to the implementation of the Anti-Money Laundering (APU) program on a regular basis.

5. References

BRI Annual Report 2022, https://bri.co.id/report, accessed 19 August 2023.

Hartono, M Dimyati. 1997. Five Steps to Building Good Government. Jakarta: Ind Hill Co.

https://complyadvantage.com/insights/how-to-prioritize-risk-during-customer-onboarding/, accessed 19 August 2023.

https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidance-for-

[27]Article 79 paragraph (2) POJK no. 8 of 2023 concerning Implementation of Anti-Money Laundering (APU) Programs, Prevention of Terrorism Financing (PPT) and Prevention of Funding for the Proliferation of Weapons of Mass Destruction (PPPSPM) in the Financial Services Sector.
[28]Article 80 paragraphs (1) and (2) POJK no. 8 of 2023 concerning Implementation of Anti-Money Laundering (APU) Programs, Prevention of Terrorism Financing (PPT) and Prevention of Funding for the Proliferation of Weapons of Mass Destruction (PPPSPM) in the Financial Services Sector.

Effective-AML-CFT-Transaction-Monitoring-Controls.pdf, accessed 21 August 2023.

Hussein, Yunus. 2004. The Crime of Money Laundering from an International Law Perspective. Jakarta: Institute for International Legal Studies, Faculty of Law, University of Indonesia.

Indonesian Bankers Association (IBI) and Banking Compliance Directors Communication Forum (FKDKP). 2018. Culture Start From The Top: Building a Culture of Compliance. Jakarta: PT Gramedia Pustaka Utama.

Interview with Mrs. Mila Mulyani as Team Leader of AML-CFT Analyst & Reporting, Compliance Division BRI, on August 09, 2023.

Regulation of the Head of PPATK Number: PER-02/1.02/PPATK/02/15 concerning Categories of Service Users Who Have the Potential to Commit the Crime of Money Laundering.

Republic of Indonesia Financial Services Authority Regulation Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Funding for the Proliferation of Weapons of Mass Destruction in the Financial Services Sector.

The FATF's RBA to AML/CFT, Financial Action Task Force's Guidance for A Risk Based Approach (RBA) – The Banking Sector October 2014.

Wahyuningsih, Sri Endah and Rismanto. 2015. Criminal Law Enforcement Policy for Combating Money Laundering in the Context of Criminal Law Reform in Indonesia. Journal of Legal Reform, Vol. II, No. January 1 – April 2015,https://jurnal.unissula.ac.id/index.php/PH/article/view/1414