SECTORAL RISK ASSESSMENT

NON-BANK PAYMENT SERVICE PROVIDERS AND NON-BANK MONEY CHANGERS

2021

BANK INDONESIA
INDONESIAN FINANCIAL TRANSACTION REPORTS AND ANALYSIS CENTRE

Contents

PART I

2

PART II

NON-BANK MONEY CHANGERS

31

PART II

NON-BANK MONEY OR VALUE TRANSFER SERVICES (MVTS)

58

PART II

NON-BANK ELECTRONIC MONEY ISSUERS AND NON-BANK ELECTRONIC WALLET SERVICE PROVIDERS

86

PART II

NON-BANK CARD-BASED PAYMENT INSTRUMENT (CBPI)

112

PART III

138

PART IV

144

PART V

152

List of Tables

PART I

PART II

PART II

PART II

PART II

PART II

PART II

List of Figures

PART I

PART II

List of Graphs

PART II

PART IV

Foreword Bank Indonesia Governor

PERRY WARJIYO
GOVERNOR OF BANK INDONESIA

"Bank Indonesia is fully committed to the prevention and eradication of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in accordance with the fourth Vision of Indonesia's Payment System Blueprint 2025, which seeks to strike an optimal balance between financial system innovation and integrity."

Praise be to God Almighty for only by His grace could the Sectoral Risk Assessment of Money Laundering (ML), Terrorist Financing (TF) and Financing of Proliferation of Weapons of Mass Destruction (PFWMD) in Non-Bank Payment Service Providers and Non-Bank Money Changers be completed.

ML, TF, and PFWMD pose a significant threat to economic stability and financial system integrity, while endangering the very foundations of community life, the state and country. Bank Indonesia is fully committed, therefore, to supporting government measures to prevent ML, TF, and PFWMD in its function as the payment system authority.

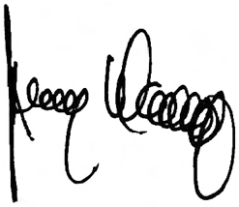
Within the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime of Indonesia, financial institutions, including non-bank payment service providers and non-bank money changers, not only assist law enforcement but also protect themselves from becoming a means or target for ML, TF, and PFWMD. To that end, a sectoral risk assessment is invaluable for financial institutions to understand, identify and measure the risk of ML, TF, and PFWMD based on four risk factors, namely customer risk, regional risk, product/service risk and delivery channel risk. In this context, Bank Indonesia enacts regulations, grants and revokes licences and permits,

implements oversight and supervision and imposes sanctions on payment service providers and money changers under the jurisdiction of Bank Indonesia in accordance with prevailing laws and regulations.

Within this regulatory and supervisory framework, I welcome the Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in Non-Bank Payment Service Providers and Non-Bank Money Changers. Through this assessment, the emerging threats and risks associated with ML, TF, and PFWMD can be mapped and mitigated, thus bolstering financial system integrity, increasing Indonesia's credibility and reputation as well as complying with international standards, including the Financial Action Task Force (FATF) recommendations.

In closing, I would like to express my utmost appreciation to all the contributors and editorial team responsible for preparing the Sectoral Risk Assessment of ML, TF, and PFWMD in Non-Bank Payment Service Providers and Non-Bank Money Changers. May God Almighty always bless and lighten our steps together.

Bank Indonesia Governor



Perry Warjiyo

PART I


CREDIT CARD

1

INTRODUCTION

A. Background/Overview

Money Laundering (ML), Terrorist Financing (TF), and Financing of Proliferation of Weapons of Mass Destruction (PFWMD) pose a significant threat to economic stability and financial system integrity, while endangering the very foundations of community life, the state and country. Indonesia, therefore, is fully committed to developing an Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime. In terms of AML/CFT regimes, the Financial Action Task Force (FATF) has issued international standards as a reference for each country in the prevention and eradication of money laundering and terrorist financing, known as the FATF 40 Recommendations.[1] In accordance with Recommendation Number 1 of the FATF, each country must identify, analyse and assess the domestic risks associated with money laundering, terrorist financing, and financing of of proliferation of weapons of mass destruction.

In 2021, Indonesia identified, analysed and assessed the latest money laundering risks using a holistic approach through the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021. The NRA in 2021 contained invaluable information concerning the risks associated with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the period from 2015-2021, domestically and internationally, as well as the latest emerging threats and outcomes of special surveillance concerning the Covid-19 impact on potential money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks and crimes in Indonesia.

Following the NRA, Indonesia also compiled a National Strategy for the Prevention and Eradication of Money Laundering and Terrorist Financing 2020-2024 (known in Indonesian as *Stranas TPPU TPPT*), containing the various risk mitigation efforts required by government ministries/agencies based on the NRA outcomes. One action plan for 2021, as contained in *Stranas TPPU TPPT*, is to update the Sectoral Risk Assessment (SRA) in Indonesia. The SRA is compiled by supervisory and regulatory bodies (LPP) as well as law enforcement agency (APH) for each sector under the respective authority. Updating the SRA is expected to comprehensively illustrate the latest sectoral risks, including the key risks, trends and typologies of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in each sector. Indonesia has already appointed government ministries/agencies as supervisory and regulatory bodies, along with the requisite tasks in accordance with the Money Laundering (ML)[2] and Terrorist Financing (TF)[3] Acts.

Bank Indonesia is fully committed to supporting government measures in Indonesia seeking to prevent money laundering, terrorist financing and financing of proliferation of weapons of mass destruction through Bank Indonesia's role as the payment system authority as well as a supervisory and regulatory body for Non-Bank Payment Service

1 The FATF 40 Recommendations are standards issued by the Financial Action Task Force (FATF), containing measures to prevent money laundering and terrorist financing through laws, financial system regulations and international cooperation.

2 Act Number 15 of 2002 concerning Money Laundering, as amended by Act Number 25 of 2003 and Act Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering.

3 Act Number 9 of 2013 concerning the Prevention and Eradication of Terrorist Financing.

Providers[4] and Non-Bank Money Changers. In this context, Bank Indonesia enacts regulations, grants and revokes licences and permits, implements supervision and imposes sanctions on payment service providers and money changers under the jurisdiction of Bank Indonesia in accordance with prevailing laws and regulations. Bank Indonesia's commitment to prevent money laundering, terrorist financing and financing of proliferation of weapons of mass destruction is also realised in the fourth vision of the Payment System Blueprint 2025, namely to strike an optimal balance between innovation, consumer protection, integrity and stability, healthy business competition through the application of Know Your Customer (KYC) principles, AML/CFT, public data and information disclosure, as well as the application of RegTech and SupTech in reporting, regulation and supervision.

Beyond its role as a supervisory and regulatory body, Bank Indonesia is also tasked with protecting the payment system industry, including non-bank money changers, from becoming a means or target for money laundering, terrorist financing and proliferation financing of WMD. As a preliminary risk mitigation measure, Bank Indonesia in conjunction with the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) has assessed and updated the latest money laundering, terrorist financing and proliferation financing risks based on customer profile, geographical region, product and service as well as delivery channel[5], as contained in the SRA 2021. Finally, SRA 2021 will be used as the basis for risk mitigation and determining the monitoring priorities of the supervisory and regulatory bodies.

B. Goals

The goals of the risk assessment concerning money laundering, terrorist financing and financing of proliferation of weapons of mass destruction for non-bank payment service providers and non-bank money changers are as follows:

1. Identifying and analysing the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

2. Identifying, analysing and evaluating various risks associated with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction based on risk mapping of **customer profiles (individual and corporate), regions, products and services as well as delivery channels**.

3. Identifying and analysing new and/or emerging threats posed by money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

4. Formulating strategy measures to mitigate the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

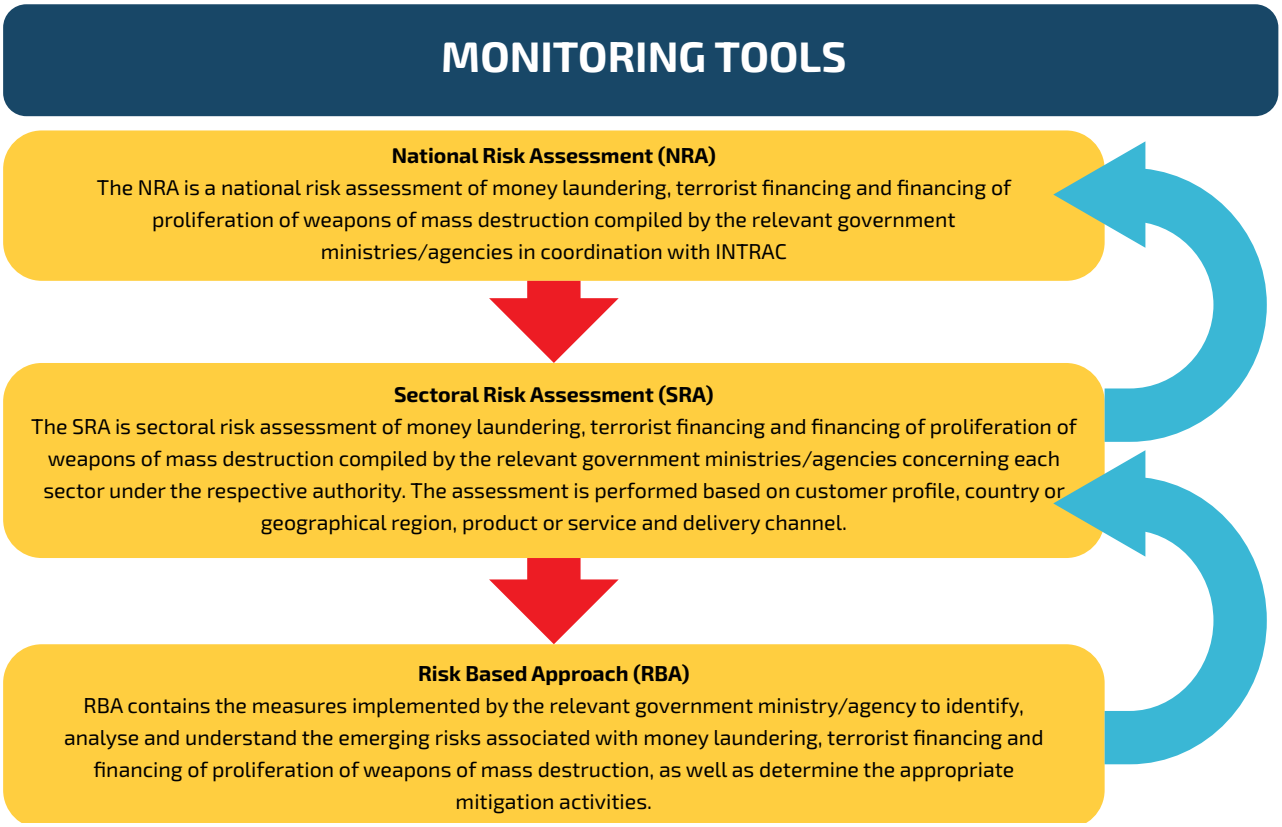
4 The term Payment Service Providers (PJP) is defined in accordance with Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System. PJP include Banks and Non-Bank Financial Institutions that provide services to facilitate payment transactions for their customers. In accordance with Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT), Non-Bank Payment Service Providers include Non-Bank Money or Value Transfer Services, Non-Bank Card-Based Payment Instrument Issuers, Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers, as also stipulated in the Money Laundering Act. According to the Money Laundering Act, Money or Value Transfer Services are Non-Bank Money or Value Transfer Services (MVTS) as stipulated in the Bank Indonesia Regulation (PBI) on AML/CFT. Referring to Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning Payment Service Providers, Non-Bank Payment Service Providers offer the following activities: (1) Account Issuance Services (AIS), (2) Payment Initiation and/or Acquiring Services (PIAS), (3) Account Information Services (AinS), (4) Data Storage Services with Access to Funding Sources in the form of Payment Instruments, and/or (5) Remittance Services.

5 A delivery channel is the customer's access point to the products and services of financial service providers.

C. Outcomes

SRA is expected to underline policymaking at Bank Indonesia and the INTRAC, specifically in relation to the regulation and supervision of AML/CFT in non-bank payment service providers and non-bank money changers. In addition, the SRA outcomes will provide guidelines for non-bank payment service providers and non-bank money changers when identifying the risks associated with business activity and taking the appropriate mitigation measures. Figure 1.1 describes the relationship between the risk assessment process.

Figure 1.1. Risk Assessment Process



2

ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM (AML/CFT) REGIME

A. AML/CFT Regime in Indonesia

The development of technology, communication and information has led to more diverse and complex transactions, which could increase the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. Currently, money laundering, terrorist financing and proliferation financing of WMD not only exploit institutions in the financial system but have also penetrated various non-financial sectors. In anticipation, the FATF has issued international standards as a reference for each country in the prevention and eradication of money laundering and terrorist financing, known as the FATF 40 Recommendations. The FATF is an independent intergovernmental body established at the G7 Summit in 1989, mandated with developing and promoting policies to protect the global financial system against money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. According to FATF Recommendation Number 1:

The prevention and eradication of money laundering in Indonesia were strengthened by the promulgation of Act Number 15 of 2002 concerning Money Laundering, as amended by Act Number 25 of 2003, and Act Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (known in Indonesia as the TPPU or Money Laundering Act). On the other hand, the eradication of terrorist financing was strengthened by the promulgation of Act Number 9 of 2013 concerning the Prevention and Eradication of Terrorist Financing (known in Indonesia as the TPPT or Terrorist Financing Act). Through those laws, Indonesia has:

1. Adjusted to the developing needs of international practices and standards,
2. Increased legal assurance for effective law enforcement, including efforts to trace and return assets as the proceeds of crime, and
3. Built public trust by maintaining financial system integrity.

Striving to prevent and eradicate money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, Bank Indonesia cooperates with various relevant stakeholders as follows:

"Countries should identify, assess and understand the risk of money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction for the country and should take action, including designating an authority or mechanism to coordinate actions to assess risk, and apply resources, aimed at ensuring the risks are mitigated effectively."

1. National Committee on the Prevention and Eradication of Money Laundering (ML Committee)

In accordance with Presidential Regulation No. 117 of 2016, as an amendment to Presidential Regulation No. 6 of 2012 concerning the National Coordination Committee on the Prevention and Eradication of Money Laundering, the National Committee on the Prevention and Eradication of Money Laundering was established to increase the effectiveness of coordination between institutions in the prevention and eradication of

money laundering. The National Committee on the Prevention and Eradication of Money Laundering has the following functions:

a. Formulate the direction, policy and strategy for the prevention and eradication of money laundering.

b. Increase coordination between institutions in relation to program and activity implementation in line with the direction, policy and strategy for money laundering prevention and eradication.

c. Coordinate the measures required to manage other matters relating to the prevention and eradication of money laundering.

d. Monitor and evaluate program and activity implementation in line with the direction, policy and strategy for money laundering prevention and eradication.

Chairman	:	Coordinating Minister for Political, Legal and Security Affairs
Deputy Chairman	:	Coordinating Minister for Economic Affairs
Secretary	:	Head of Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)
Members	:	

1. Minister of Foreign Affairs
2. Minister of Home Affairs;
3. Minister of Finance;
4. Minister of Law and Human Rights;
5. Minister of Trade;
6. Minister of Cooperatives and SMEs;
7. Governor of Bank Indonesia;
8. Chairman of OJK Board of Commissioners;
9. Attorney General;
10. Chief of Indonesian National Police;
11. Chief of State Intelligence Agency;
12. Chief of National Counter-Terrorism Agency; and
13. Chief of National Narcotics Board

Implementation Team :

Chairman :

Head of Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)

Deputy Chairman :

Deputy for Coordination of Law and Human Rights, Coordinating Ministry for Political, Legal and Security Affairs

Members :

1. Deputy for Coordination of Law and Human Rights, Coordinating Ministry for Political, Legal and Security Affairs;
2. Deputy for Coordination of International Economic Cooperation, Coordinating Ministry for Economic Affairs;
3. Deputy Governor of Bank Indonesia for the Payment System and Rupiah Currency Management, Bank Indonesia;
4. Head of the Commodity Futures Trading Regulatory Agency
5. Deputy Assistant of Financing and Guarantees, Ministry of Cooperatives and SMEs
6. Deputy Assistant of Supervision, Ministry of Cooperatives and SMEs;
7. Executive Head of Banking Supervision, Financial Services Authority (OJK);
8. Director General of Customs and Excise, Ministry of Finance;
9. Director General of Taxes, Ministry of Finance;
10. Director General of State Assets, Ministry of Finance;
11. Secretary General, Ministry of Finance;

12. Director General of Multilateral Cooperation, Ministry of Foreign Affairs;
13. Director General of Law and International Agreements, Ministry of Foreign Affairs;
14. Director General of Legal Administrative Affairs, Ministry of Law and Human Rights;
15. Director General of Immigration, Ministry of Law and Human Rights;
16. Director General of Politics and Public Administration, Ministry of Home Affairs;
17. Directorate General of Population and Civil Registration, Ministry of Home Affairs;
18. Deputy Attorney General on General Criminal Affairs, Attorney General of the Republic of Indonesia;
19. Deputy Attorney General on Special Criminal Affairs, Attorney General of the Republic of Indonesia;
20. Chief of Criminal Investigation Agency, Indonesian National Police;
21. Commander of Counterterrorism Special Detachment (Densus) 88, Indonesian National Police;
22. Deputy for Enforcement and Capacity Building, National Counter-Terrorism Agency;
23. Deputi Penindakan dan Pembinaan Kemampuan Badan Nasional Penanggulangan Terorisme; dan
24. Deputy of Eradication, National Narcotics Board

Seeking to coordinate and ensure the effectiveness of efforts to prevent and eradicate money laundering, terrorism financing and financing of proliferation of weapons of mass destruction, the National Committee on the Prevention and Eradication of Money Laundering formulated a National Strategy (*Stranas*) for the Prevention and Eradication of Money Laundering and Terrorist Financing. The national strategy is used as a reference for government ministries and agencies under the auspices of the National Committee on the Prevention and Eradication of Money Laundering, as well as other relevant parties when formulating programs and implementing activities in line with the direction, policy and strategy for the

Figure 1.2. National Strategy for the Prevention and Eradication of Money Laundering and Terrorist Financing

prevention and eradication of money laundering, terrorism financing and proliferation financing of WMD. Since 2007, the National Committee on the Prevention and Eradication of Money Laundering has implemented the national strategy through four consecutive periods as figure presented above.

2. Reporting Parties

According to Article 1 of the Money Laundering Act, a Reporting Party is any individual legally obliged to submit reports to the INTRAC. In practice, INTRAC has expanded the scope of Reporting Parties in accordance with Paragraph (1), Article 17 of the Money Laundering Act, Elucidation of the Money Laundering Act as well as Article 2 and Article 8 of Government Regulation Number 61 of 2021, as an amendment to Government Regulation Number 43 of 2015 concerning the Reporting Parties in the Prevention and Eradication of Money Laundering. Reporting parties consist of the following:

a. Financial Services Providers

1. Banks
2. Finance companies
3. Insurance companies and brokers
4. Pension funds
5. Securities companies
6. Investment managers
7. Custodians
8. Trustees
9. Postal companies as providers of money transfer services
10. Money changers
11. Card-Based Payment Instrument Issuers
12. Electronic Money Issuers and Electronic Wallet Service Providers
13. Savings and loans cooperatives
14. Pawnbrokers
15. Commodity futures trading service providers
16. Remittance service providers
17. Venture capital companies
18. Infrastructure financing companies
19. Microfinance institutions
20. Export financing institutions
21. Online/peer-to-peer lenders
22. Crowdfunding service providers
23. FinTech financial transaction service providers

b. Providers of goods and/or other services (GSP)

1. Estate agents
2. Motor vehicle dealers
3. Gems, jewellery and precious metal dealers
4. Art and antique dealers
5. Auction houses

c. Professional services

1. Advocates
2. Notaries
3. Land deed officials (PPAT)
4. Accountants
5. Public accountants
6. Financial planners

3. Supervisory and Regulatory Bodies

Point 17 of Article 1 of the Money Laundering Act and Point 12 of Article 1 of the Terrorist Financing Act stipulates that Supervisory and Regulatory Bodies (LPP) are those authorised to supervise, regulate and/or sanction a Reporting Party. Among government ministries/agencies, Bank Indonesia, the Financial Services Authority (OJK), INTRAC, Ministry of Cooperatives, Ministry of Trade and the Ministry of Finance are authorised as supervisory and regulatory bodies (LPP). The jurisdiction of LPP is as follows:

a. Establishing customer due diligence principles.
b. Supervising compliance of Reporting Parties to customer due diligence principles.
c. Imposing administrative sanctions on reporting parties for failure to report financial transactions.
d. Supervising compliance to reporting obligations by reporting parties
e. Establishing procedures to supervise compliance

4. Public

The public plays an essential role in the prevention and eradication of money laundering, terrorism financing and financing of proliferation of weapons of mass destruction. Within an AML/CFT regime, the public can play an active role in providing information to the INTRAC, law enforcement agency and other relevant parties concerning money laundering, terrorism financing and proliferation financing of WMD.

B. AML/CFT Regime in Bank Indonesia

Indonesia Payment System (SPI) 2025[6] strikes an optimal balance between payment system innovation and integrity through the application of anti-money laundering and combating the financing of terrorism and financing of proliferation of weapons of mass destruction in line with Vision 4 of the Indonesia Payment System Blueprint 2025 as follows: "SPI 2025 guarantees balance between innovation and consumer protection, integrity and stability, as well as healthy business competition through the application of Know Your Customer (KYC) principles as well as an anti-money laundering and combating the financing of terrorism regime, public data/information disclosure, the application of regulatory technology (RegTech) and supervisory technology (SupTech) for reporting obligations, regulation and supervision."

1. Policy and Risk Analysis

The Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Framework was developed to support the Vision of SPI 2025 and prevent money laundering, terrorism financing and financing of proliferation of weapons of mass destruction, which can pose various threats as follows:

a. Threatening economic stability and financial system integrity.
b. Reducing Indonesia's credibility in the eyes of the international community.
c. Increasing investment risk.
d. Threatening national sovereignty by financing terrorists.

The achievements of AML/CFT implementation in the SPI are as follows:

a. National financial system integrity in Indonesia supporting economic stability.
b. Stronger national credibility and reputation in the eyes of the international community through compliance to international standards.
c. National financial system integrity in Indonesia supporting the investment climate.
d. Terrorist actions mitigated by combating the financing of terrorism.

As a supervisory and regulatory body (LPP), Bank Indonesia has issued various regulations and guidelines concerning AML/CFT. In 2017, Bank Indonesia promulgated Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 regarding the Application of Anti-Money Laundering and combating the financing of terrorism for Non-Bank Payment Service Providers and Non-Bank Money Changers (known as PBI AML/CFT).

6 Indonesia Payment System Blueprint (BSPI) 2025 contains the direction of Bank Indonesia payment system policy to navigate the payment system industry in the digital economy and finance era through five Indonesia Payment System Visions for 2025. BSPI 2025 is accessible via https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx

Figure 1.3. AML/CFT Framework in Bank Indonesia

Source: Bank Indonesia

The provisions contained in the Bank Indonesia Regulation on Anti-Money Laundering and Combating The Financing of Terrorism have been enforced since September 2017 for non-bank payment service providers, namely non-bank money or value transfers services providers, issuers of card-based payment instruments, issuers of electronic money and e-wallet providers as well as non-bank money changers. The regulation clearly stipulates the AML/CFT obligations for non-bank payment service providers[7] and non-bank money changers as follows:

a. Roles and responsibilities of the Directors and active supervision of the Board of Commissioners.
b. Policies and written procedures.
c. Risk management process.
d. Management of human resources.
e. Internal control system.

In addition to issuing the Bank Indonesia Regulation on Anti-Money Laundering and Combating the Financing of Terrorism for Non-Bank Payment Service Providers and Non-Bank Money Changers (PBI AML/CFT), Bank Indonesia also issued other regulations referring to the PBI AML/CFT as follows:

a. Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning Payment Service Providers (PJP) (known as PBI PJP).
b. Bank Indonesia Regulation (PBI) No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PIP) (known as PBI PIP).

7 According to the Bank Indonesia Regulation on Anti-Money Laundering and Combating the Financing of Terrorism for Non-Bank Payment Service Providers and Non-Bank Money Changers (PBI AML/CFT), non-bank payment service providers include non-bank money or value transfer service providers, issuers of card-based payment instruments, issuers of electronic money and e-wallet providers.

In addition, Bank Indonesia also issued technical guidelines relating to the PBI AML/CFT as follows:

a. Risk-based approach AML/CFT implementation guidelines.

b. Customer due diligence principles for Non-Bank Payment Service Providers and Non-Bank Money Changers.

c. Implementation guidelines to immediately block or freeze funds belonging to individuals or corporations identified on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).

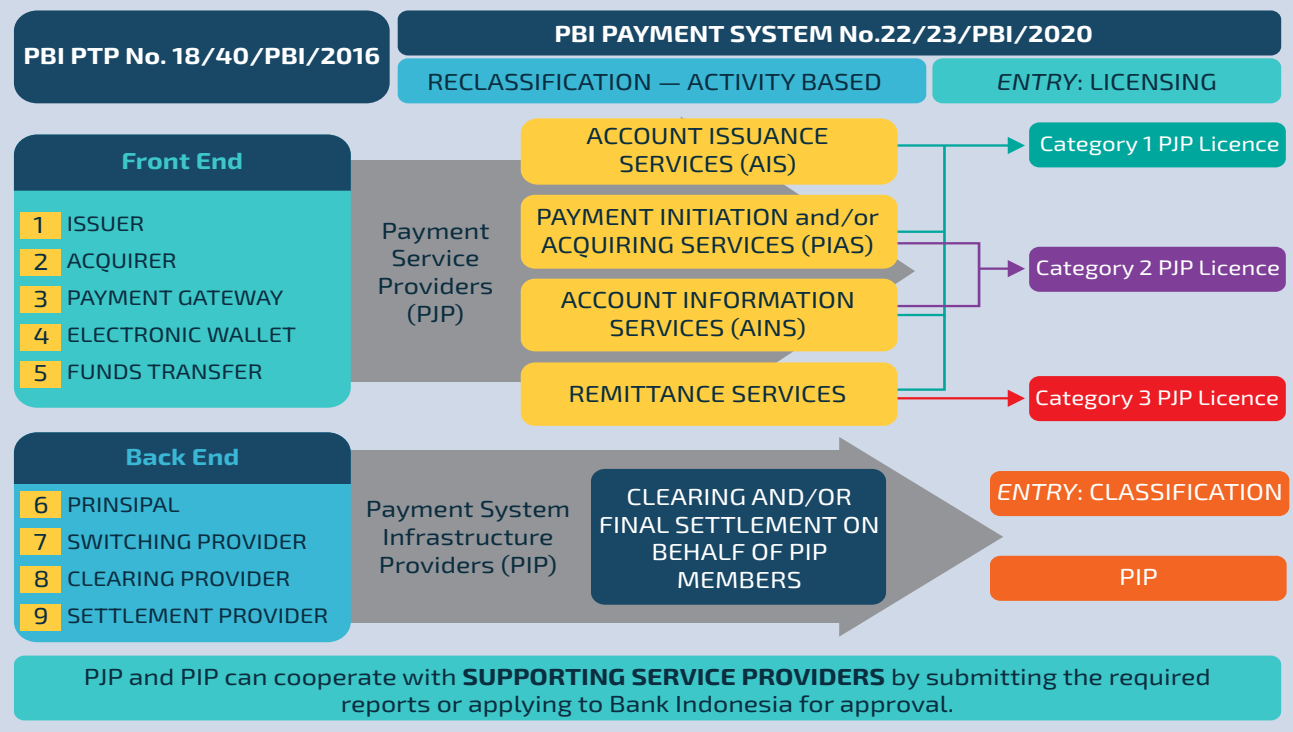
d. Implementation guidelines to immediately block or freeze funds belonging to individuals or corporations identified on the Proliferation Financing List.

2. Licensing

As stipulated in Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System, Parties eligible to operate as Payment Service Providers (PJP) are Banks and Non-Banks licensed by Bank Indonesia.

Licences for Payment Service Providers (PJP) are granted based on licence category or activity bundling, supported by robust business processes, mechanisms and licensing requirements to regulate the payment system industry. The licensing process consists of various stages, including an administrative assessment, substantive analysis of application documents and on-site visits. Licences to perform PJP activities are based on the following categories:

Figure 1.4. Reclassification of Payment System Providers



Source: Bank Indonesia

a. Category 1 PJP Licence

1. Account Issuance Services (AIS)
2. Payment Initiation and/or Acquiring Services (PIAS)
3. Account Information Services (AinS)
4. Remittance Services

b. Category 2 PJP Licence

1. Account Information Services (AinS)
2. Payment Initiation and/or Acquiring Services (PIAS)

c. Category 3 PJP Licence

1. Remittance Services
2. Other services stipulated by Bank Indonesia

3. Supervision

In terms of supervision, Bank Indonesia applies a risk-based approach to supervising AML/CFT implementation by Payment Service Providers (PJP) as a continuous activity involving the processes of identification, monitoring and risk assessment. In the application of a risk-based approach (RBA), Bank Indonesia has formulated RBA guidelines referring to the Sectoral Risk Assessment (SRA) as a guide for supervisors and payment service providers in the identification, assessment and understanding of risks associated with money laundering, terrorism financing and financing of proliferation of weapons of mass destruction.

4. Enforcement

Bank Indonesia coordinates closely with law enforcement, specifically the Indonesian National Police, predominantly to control unlicensed non-bank money changers and illegal money or value transfer service providers. Such measures aim to mitigate the risks associated with money laundering, terrorism financing and financing of proliferation of weapons of mass destruction, with the involvement of all Bank Indonesia Representative Offices. Between March 2017 and December 2021, Bank Indonesia in conjunction with the Indonesian National Police identified and took punitive action against 1,090 non-bank money changers and 79 illegal money or value transfer service providers. The action was recognised by the Indonesia APG Mutual Evaluation Team in 2017 as the most significant sanctions imposed by any Indonesian authority.

5. Domestic and International Cooperation

Strengthening AML/CFT implementation and safeguarding the financial system from exploitation as a means of money laundering, terrorism financing and financing of proliferation of weapons of mass destruction, Bank Indonesia actively and continuously coordinates with other relevant authorities, including the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), Indonesian National Police (POLRI), National Narcotics Agency (BNN), Corruption Eradication Commission (KPK), Financial Services Authority (OJK) and Ministry of Finance (MoF). The forms of domestic cooperation to prevent and eradicate money laundering, terrorism financing and proliferation financing of WMD are as follows:

a. Signing memorandums of understanding (MoU)
b. Exchanging data and information
c. Joint supervisions
d. Training and/or exchanging resources
e. Employee secondments
f. Task force participation, such as the DTTOT Task Force

In addition, Bank Indonesia also actively cooperates with other central banks, including Bank Negara Malaysia (BNM), Bank of Thailand (BoT), Bangko Sentral Ng Pilipinas (BSP), Brunei Darussalam Central Bank (BDCB), Central Bank of United Arab Emirates (CBUAE) and Monetary Authority of Singapore (MAS). In terms of

multilateral cooperation, Indonesia has been an active member of the Asia/Pacific Group on Money Laundering since 2001.

The purview of AML/CFT cooperation with foreign authorities covers the following:

a. Exchanging information and experiences concerning inter-authority policies, including AML/CFT policy.
b. Exchanging general information, such as macroeconomic policy, and specific information, such as illegal money or value transfer service providers, and AML/CFT.
c. Supervision.
d. Establishing task forces.
e. Actions against unlicensed financial institutions
f. Capacity building

6. Communication and Education

Bank Indonesia actively runs campaigns to educate the public concerning the risks of money laundering, terrorism financing and financing of proliferation of weapons of mass destruction. Public education campaigns by Bank Indonesia urge and encourage members of the public to use licensed non-bank payment service providers and non-bank money changers. Targeting payment service providers, Bank Indonesia has communicated the obligations to reject transactions without valid identification, detect suspicious financial transactions and report transactions to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC). Educational activities are provided through various channels, including print media, social media as well as face-to-face meetings with payment service providers and members of the public.

Figure 1.5. Communication and Education

Source: Bank Indonesia

C. Development of New Technologies and Technology-Based Payment Service Providers

In accordance with the Currency Act (No. 7) of 2011, currency is the money issued by the Republic of Indonesia, known as rupiah. Based on the Currency Act, Bank Indonesia has stipulated that virtual currencies are not recognised as legal tender and prohibited as a means of payment in the territory of the Republic of Indonesia.[8]

Since July 2021, payment system regulations have been administered in accordance with Bank Indonesia Regulation No. 22/23/PBI/2020 concerning the Payment System (PBI SP), Bank Indonesia Regulation No. 23/6/PBI/2021 concerning Payment Service Providers (PBI PJP) and Bank Indonesia Regulation No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PBI PIP). Upon enactment of PBI SP, the existing PBI PTP[9], PBI Tekfin[10], PBI UE[11] and PBI APMK[12] were repealed in their entirety. Notwithstanding, the implementation guidelines of the four repealed regulations remained valid and effective for up to one year from the promulgation date of Bank Indonesia Regulation No. 23/6/PBI/2021 concerning Payment Service Providers (PBI PJP), providing no regulatory conflict with PBI PJP.

The provisions contained within PBI SP, PBI PJP, and PBI PIP relating to the development of new technologies and technology-based payment service providers are as follows:

1. Payment Service Providers (PJP) are Banks or Non-Banks providing services to facilitate payment transactions for customers. PJP offering the following activities: (a) Account Issuance Services (AIS), (b) Payment Initiation and/or Acquiring Services (PIAS) (c) Account Information Services (AinS), and/or (d) Remittance Services, must be licensed by Bank Indonesia in accordance with prevailing regulations.
2. Payment System Infrastructure Providers (PIP) are entities that administrate payment system infrastructure as a means to transfer funds on behalf of the members. PIP engage in the following activities: (a) Clearing, and/or (b) Final Settlement.
3. PJP and PIP are required to fulfil general payment system principles, including prevailing laws and regulations on Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT).
4. Bank Indonesia prohibits the use of virtual currencies as a payment instrument in Indonesia in accordance with:
    a. Article 2 of Bank Indonesia Regulation (PBI) No. 17/3/PBI/2015 concerning Mandatory Rupiah Use in the Territory of the Republic of Indonesia, stipulating that all parties are obligated to use the rupiah for transactions within the territory of the Republic of Indonesia, including all cash and cashless payment transactions.
    b. Article 73, Letter b of Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System, stipulating that Bank Indonesia can formulate regulations on restrictions for PJP and PIP against receiving, using, connecting and/or processing payment transactions using virtual currencies.

---

8 The announcement was made via Press Release No. 20/4/DKom, dated 13th January 2018, entitled Bank Indonesia Warns all Parties Not to Sell, Buy or Trade Virtual Currency.

9 Bank Indonesia Regulation (PBI) No. 18/40/PBI2016 concerning Payment Transaction Processing.

10 Bank Indonesia Regulation (PBI) No. 19/12/PBI/2017 concerning FinTech.

11 Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money.

12 Bank Indonesia Regulation (PBI) No. 14/2/PBI/2021, as an amendment to PBI No. 11/11/PBI/2009 concerning Card-Based Payment Instruments.

c. Article 202 of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning Payment Service Providers (PJP), stipulating that PJP are prohibited from:

   i. Receiving virtual currencies as a source of funds in processing payment transactions.

   ii. Processing payment transactions using virtual currencies as a source of funds.

   iii. Connecting virtual currencies with payment transaction processing.

d. Article 203 of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning PJP, stipulating that Payment Service Providers (PJP) are prohibited from facilitating the trade of virtual currencies as a commodity, unless stated in prevailing laws and regulations.

e. Article 204, Paragraph (1), Letter b of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning PJP, stipulating that value, as it pertains to money, cannot be met by sources of funds as referred to in Article 144, including digital currencies issued by parties other than the monetary authority (virtual currency) with the following characteristics:

   i. Expressed in units.

   ii. Using cryptography and distributed ledgers or other sophisticated technologies to regulate the creation of new units and the transaction processing mechanisms.

   iii. Used for payment purposes or to fulfil economic activity.

   iv. Electronically transferable, storable and tradable.

   v. Fulfilling other characteristics determined by Bank Indonesia.

f. Article 152 of Bank Indonesia Regulation (PBI) No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PIP), stating that PIPs are not permitted to:

   i. Receive virtual currencies used as a source of funds to process payment transactions,

   ii. Process payment transactions using virtual currencies as a source of funds,

   iii. Connect virtual currencies with payment transaction processing, and/or

   iv. Facilitate trading of virtual currencies as a commodity, unless regulated in accordance with prevailing laws and regulations.

5. Bank Indonesia provides a sandbox to facilitate trials for payment system technology development and innovation as follows:

   a. Providing a sandbox to facilitate trials and support development of the digital economy and finance.

   b. The scope of payment system technology innovation includes the products, activities, services and business models using innovative technologies in a digital economic and financial ecosystem to support the payment system.

   c. Implementing trials for payment system technology development as an innovation lab for new products and services, a regulatory sandbox for new policies and regulations and an industrial sandbox to expand new payment system industry innovations for broader use.

D. Sectoral Risk Assessment of Money Laundering and Terrorist Financing in 2019

Bank Indonesia conducted a risk assessment of money laundering and terrorist financing among non-bank payment service providers and non-bank money changers in 2019 based on customer profile, region, product or service as well as delivery

channel. The risk assessment was contained in a Sectoral Risk Assessment (SRA), referring to the National Risk Assessment (NRA) of Money Laundering and Terrorist Financing. The goals of the SRA are stated as follows:

1. Identifying and analysing emerging risks and vulnerabilities concerning money laundering and terrorist financing.

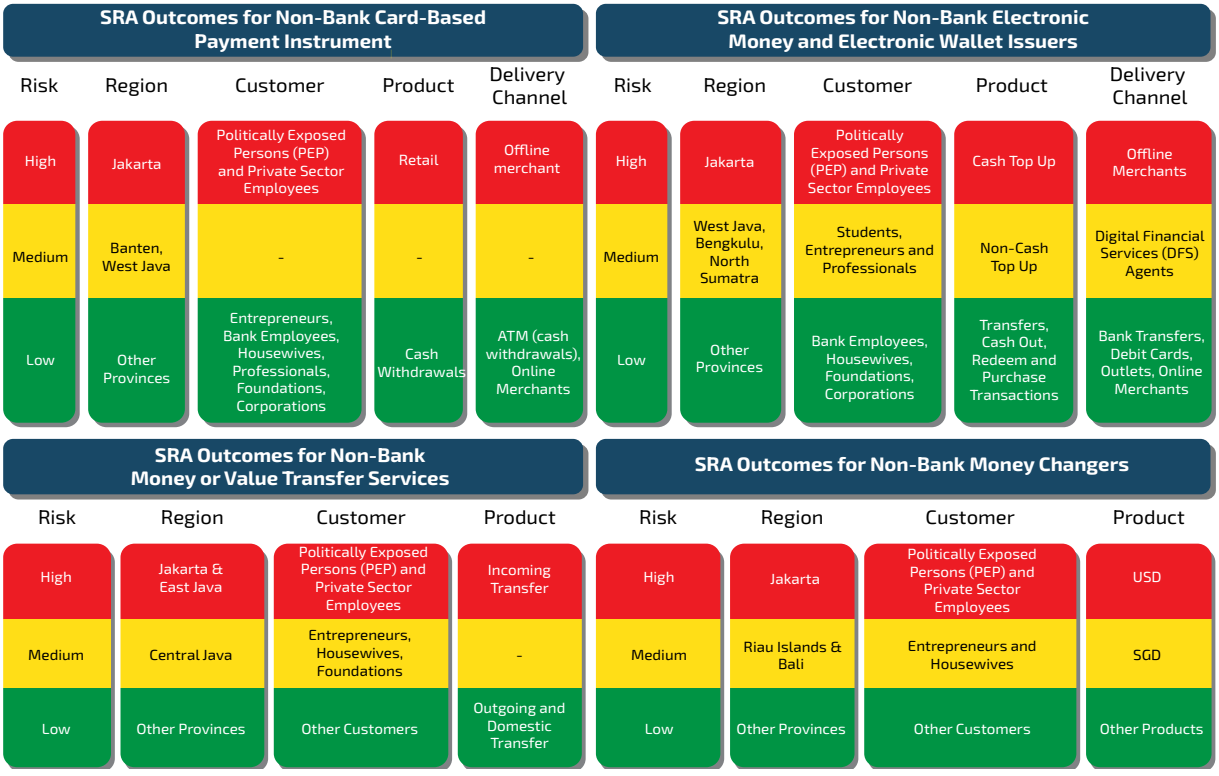
2. Analysing the key risks of money laundering and terrorist financing, including mapping the risks based on customer profile, region, product or service as well as delivery channel.

The outcomes of the Sectoral Risk Assessment of Money Laundering and Terrorist Financing in 2019 are as follows:

E. National Risk Assessment of Money Laundering and Terrorist Financing 2021

One instrument to effectively prevent and eradicate money laundering, terrorism financing and financing of proliferation of weapons of mass destruction is the National Risk Assessment (NRA) of Money Laundering, Terrorism Financing and Financing of Proliferation of Weapons of Mass Destruction. Through the NRA, stakeholders can acquire greater understanding of the money laundering risks based on risk level. Seeking to bring up to date the latest money laundering developments, the Government of the Republic of Indonesia, under the auspices of the National Money Laundering Committee, updated the 2015 NRA. In 2021, Indonesia published the Indonesia Risk Assessment of Money Laundering, Terrorism Financing and financing of proliferation of weapons of mass destruction, which identified the risks and mitigation efforts in Indonesia from 2016-2020. Based on the risk identification and mitigation plan

Figure 1.6. Outcomes of the Sectoral Risk Assessment of Money Laundering and Terrorist Financing in 2019



Source: Bank Indonesia

implemented by Indonesia, the NRA recommended several priority actions, such as strengthening RBA implementation as well as domestic and international cooperation, both formal and informal.

1. NRA of Money Laundering in 2021

The typologies of money laundering have evolved in Indonesia to become more complex and varied. Money laundering can exploit financial institutions and non-financial institutions. Based on the outcome of the National Risk Assessment (NRA) of Money Laundering, cases in Indonesia are dominated by the predicate offences of narcotics and corruption. Perpetrators also exploit automotive dealerships, estate agents, commercial banks and non-bank money changers to conceal their financial activity. Meanwhile, most money laundering criminals are employed as government/legislative officials, employees of state/regional-owned enterprises, or business entities incorporated as limited liability companies. The highest risk region for money laundering is Jakarta, with the typologies dominated by use of false identification, nominees, trusts, family members or third parties, estate agents, smurfing[13], structuring[14], using professional services, using new payment methods/systems, using legal persons and exploiting unregulated sectors.

Furthermore, mapping the foreign inward risk or Foreign Predicate Crime (FPC)[15] based on the NRA showed that fraud, corruption, funds transfers, narcotics, electronic information and transactions (EIT) or cybercrime are the highest risk predicate offences of money laundering in Indonesia. Meanwhile, the highest risk countries of origin in terms of predicate crimes are Malaysia, Japan, Singapore, Thailand, Saudi Arabia and the United Arab Emirates. Based on individual customer profile, entrepreneurs, private sector employees, merchants, housewives, professionals and consultants, students, civil servants (including retirees) as well as lecturers/professors are considered high risk. In terms of business segment, industry and distribution were shown to be high-risk categories for foreign predicate crime (FPC).

Mapping the foreign outward risk or laundering offshore revealed that corruption and narcotics are categorised as high-risk foreign predicate crimes. High-risk destination countries of laundering offshore include Singapore, United States, India, China, Thailand, Malaysia and Hong Kong. Based on individual customer profile, government/legislative officials, entrepreneurs and private sector employees were included in the high-risk category for laundering offshore. In terms of business segment, industry is a high-risk category for laundering offshore.

13 Smurfing is a money-laundering technique involving the use of several different accounts on behalf of one customer.

14 Structuring is a money-laundering technique using relatively small, yet high-frequency, transactions in the financial sector.

15 Foreign inward risk or foreign predicate crime is money laundering in Indonesia with the predicate offences perpetrated abroad.

Table 1.1. Risk Factor Analysis based on NRA of Money Laundering in 2021

No	Category	NRA of Money Laundering 2021	
		High Risk	Medium Risk
	DOMESTIC RISKS		
1	Predicate Crime	Corruption, Narcotics	Tax Crimes, Banking Crimes, Illegal Logging, Fraud, Environmental Crimes
2	Sectors	Automotive Dealerships, Real Estate Agents, Commercial Banks, Money Changers	Money or value transfer service providers, Rural Banks
3	Perpetrators	(Non-individual) legal entities or corporations, individuals	-
4	Legal Arrangements	Limited Liability Company (PT)	Government Institutions, Foundations, Non-MSME Limited Partnership Companies, Non-MSME Partnership Firms, Cooperatives, Associations, Other Non-MSME Companies
5	Individual Customer Profile	Government/Legislative Officials, Employees of State/Regional-Owned Enterprises (including retirees)	Entrepreneurs, Private Sector Employees, civil servants (including retirees), Professionals dan Consultants, Army/Police Personnel (including retirees), Bank Employees
6	Region	Jakarta	East Java, West Java, Central Java, North Sumatra, Bali
7	Money Laundering Typologies	Use of false identification, nominees, trusts, family members or third parties, property/real estate, including property agents, smurfing[17], structuring[18], using professional services, using new payment methods/systems, using legal persons and exploiting unregulated sectors	Use of non financial institutions, money changers, mingling[19], credit cards, cheques, trade credit, trade-based money laundering and transfer pricing, jewellery and precious metal trade, illegal banks/ alternative fund transfer services, hawala, virtual currencies, valuable asset purchases (artwork, antiques, etc), Use of offshore banks, international businesses and offshore trusts, shell companies for the illicit proceeds of crime in the tax sector as well as online gambling.
	INTERNATIONAL RISKS		
	Foreign Inward Risk[20]		
8	Predicate Crime	Fraud, Corruption, Funds Transfers, Narcotics, Electronic Information and Transactions (EIT) or Cybercrime	Tax Crimes, Customs, Bribery, Malfeasance, Duties, Psychotropics, Capital Market
9	Country of Origin	Malaysia, Japan, Singapore, Thailand, Saudi Arabia, United Arab Emirates	United States, Cambodia, Jordan, Laos

16 Smurfing is a money-laundering technique involving the use of several different accounts on behalf of one customer.

17 Structuring is a money-laundering technique using relatively small, yet high-frequency, transactions in the financial sector.

18 Mingling is a money-laundering technique involving the consolidation of illicit funds in legal business activities.

19 Foreign inward risk or foreign predicate crime is money laundering in Indonesia with the predicate offences perpetrated abroad.

No	Category	NRA of Money Laundering 2021	
		High Risk	Medium Risk
10	Individual Customer Profile	Entrepreneurs, Private Sector Employees, Merchants, Housewives, Professionals and Consultants, Students, Civil Servants (including retirees), Lecturers/Professors	BUMN/BUMD Employees (including retirees), Army/ Police Personnel (including retirees), Farmers and Fishermen, Labor, Domestic Helpers, Security Personnel, Government/Legislative Officials, Artisans
11	Corporate Customer Profile	Industry and Distribution	Exports/Imports, Public Transport, Mining, Retail Trade, Consultants, Farmers, Real Estate, Electricity Supply, Travel Agents, Construction, Forestry and Logging, Fishing, Accommodation and Food Service Activities
		Foreign Out-ward Risk[21]	
12	Predicate Crime	Corruption and Narcotics	Fraud, Tax Crimes, Bribery, Banking Crimes, Customs, Migrant Smuggling, Human Trafficking, Other Crimes Punishable by a Custodial Sentence of Four Years or More
13	Destination Country	Singapura, USA, India, China, Thailand, Malaysia and Hong Kong	Australia, Japan, Taiwan
14	Individual Customer Profile	Government/Legislative Officials, Entrepreneurs and Private Sector Employees	Housewives, Merchants, Lecturers/Professors, Employees, State/Regional-Owned Enterprises (including retirees), Civil Servants (including retirees, Army/Police Personnel (including retirees), Students
15	Corporate Customer Profile	Industry	Distribution, Retail Trade, Exports/Imports, Public Transport, Mining, Construction

Source: NRA of Money Laundering 2021

20 Foreign outward risk is money laundering offshore with the predicate offences committed in Indonesia.

2. NRA of Terrorism Financing and Financing of Proliferation of Weapons of Mass Destruction in 2021

In the context of terrorist financing, the modus operandi, or typologies, are becoming more varied through conventional and virtual channels. Terrorist financing and Financing of Proliferation of Weapons of Mass Destruction (WMD) exploit financial and non-financial institutions. Based on the National Risk Association (NRA) of terrorist financing and financing of proliferation of weapons of mass destruction, terrorist financing is dominated by three typologies as follows:

1. Fundraising by terrorist financiers, funds embezzled from donations through community organisations and legitimate businesses.
2. Money transfers through financial services providers, carrying cash across borders and using new payment methods.
3. Utilising funds to purchase arms and explosives, training in the manufacture of arms and explosives, as well as travel expenses to and from acts of terrorism.

Based on customer profile, those most at risk of funding terrorists include entrepreneurs, private sector employees and merchants. Meanwhile, the highest risk areas are Jakarta, East Java, West Java and Central Java. In line with the rapid development of technology and new ways for criminals to operate that are harder to detect, the emerging threats associated with terrorist financing are as follows:

1. Financing that uses or misuses corporations/legal entities
2. Narcotics
3. Virtual assets
4. Online loans
5. Activities of armed criminal gangs in the country

Risk Factor Analysis based on the NRA of Terrorist Financing in 2021 is presented in Table 1.2.

Table 1.2. Risk Factor Analysis based on NRA of Terrorist Financing and Financing of Proliferation of WMD in 2021

No	Category	NRA of Terrorist Financing and Financing of Proliferation of WMD 2021	
		High Risk	Medium Risk
	DOMESTIC RISKS		
1	Terrorist Financing Typology: Fundraising	Fundraising by Terrorist Financiers, Funds Embezzled from Donations through Community Organisations	Legitimate businesses
2	Terrorist Financing Typology: Money Transfers	Through Financial Services Providers	Carrying Cash Across Borders and Using New Payment Methods
3	Terrorist Financing Typology: Utilising Funds	• **Domestic Terrorist Operations** (Purchasing arms and explosives, Travel expenses to and from acts of terrorism); • **International Terrorist Operations** (Travel for Foreign Terrorist Fighters – FTF); • **Training** (Manufacturing arms and explosives); • **Salaries and Compensation for Members of Terrorist Groups** (Compensation for jailed and deceased members)	• **Salaries and Compensation for Members of Terrorist Groups** • **Domestic Terrorist Operations – Basic Cost-of-Living Expenses** (Food, housing, medical costs) • **Propaganda and Recruitment** (Creating and maintaining social media accounts)

No	Category	NRA of Terrorist Financing and Financing of Proliferation of WMD 2021	
		High Risk	Medium Risk
4	Sectors	Commercial banks, money or value transfer service providers, non-bank money changers	Rural banks (BPR), Cooperatives
5	Region	Jakarta, West Java, East Java, Central Java	Central Sulawesi, Papua, Banten, West Papua
6	Individual Customer Profile	Entrepreneurs, Private Sector Employees, Merchants	Government/Legislative Officials, Political Party Leaders, Civil Servants (including retirees), Employees of State/Regional-Owned Enterprises (including retirees), Housewives, Army/Police Personnel (including retirees)
7	Corporate Customer Profile	Non-MSME limited liability companies, foundations, Associations, Non-MSME Limited Partnership Companies, Non-MSME Partnership Firms	MSMEs, Government Institutions, Other Non-MSMEs, Cooperatives
	INTERNATIONAL RISKS		
8	Foreign In-ward[21]	USA, Malaysia, Philippines, Australia	Afghanistan
9	Foreign Out-ward[22]	Malaysia, Philippines, Australia	USA, Singapore

Source: NRA of Terrorist Financing and Financing of Proliferation of WMD 2021

In the context of financing of proliferation of weapons of mass destruction, no direct threats have been identified in Indonesia. Notwithstanding, emerging threats of WMD proliferation financing in Indonesia have been identified in terms of trade transactions with countries included in a United Nations Security Council resolution. Another emerging threat is posed by the accounts of foreign nationals from high-risk countries based on the UN Security Council resolution who no longer live or work in Indonesia and are susceptible to misuse by other parties.

21 Foreign inward risk is foreign financing used for terrorist activity in Indonesia.

22 Foreign outward risk is domestic financing used for terrorist activity in foreign.

3

SECTORAL RISK ASSESSMENT METHODOLOGY

A. Research Methodology

The research methodology used when preparing the Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in 2021 combined quantitative and qualitative approaches. Quantitative data was collected and analysed using statistical data from court reports, as well as a survey issued to services providers and law enforcement agencies. On the other hand, qualitative data was collected and analysed through Focus Group Discussions (FGD) with payment service providers and relevant government ministries/agencies, coupled with a literature review. The same methods were employed when preparing the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in 2021.

The FATF guidelines on National Money Laundering and Terrorist Financing Risk Assessment were used when preparing the Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction. The same FATF guidelines were used when preparing the Sectoral Risk Assessment of Money Laundering and Terrorist Financing in 2019.

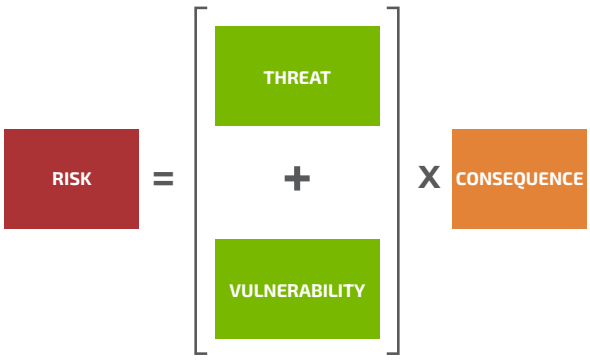
B. Scope and Framework

The sectoral risk assessment for non-bank payment service providers and non-bank money changers covers four key risks as the focus of efforts to prevent and eradicate money laundering and terrorist financing as follows:

Meanwhile, the Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in Non-Bank Payment Service Providers and Non-Bank Money Changers in 2021 also covers the domestic and international risks referring to the National Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in 2021.

The Sectoral Risk Assessment Framework refers to the FATF guidelines on National Money Laundering and Terrorist Financing Risk Assessment as general guidelines, stating that risk can be viewed as a function of three factors: threat, vulnerability and consequence. Based on those guidelines, the equation for the money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risk assessment can be expressed as follows:

Figure 1.7. Risk Assessment Framework



Source: NRA of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021

The results of the risk assessment are based on analysis of the threats, vulnerabilities and consequences, with each factor defined as follows:

1. A **threat** is a person or group of people, object or activity with the potential to cause harm to the state, society or economy. In the context of money laundering, terrorist financing and

financing of proliferation of weapons of mass destruction, this includes criminals, criminal organisations, terrorist groups and their facilitators, their funds as well as past, present or future activities.

2. The concept of **vulnerabilities** as used in the risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the context of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, vulnerabilities illustrate weaknesses in the anti-money laundering and Combating the Financing of Terrorism (AML/CFT) regime in terms of the reporting parties.

3. **Consequence** refers to the impact or harm that money laundering, terrorist financing and financing of proliferation of weapons of mass destruction may cause in the anti-money laundering and Combating the Financing of Terrorism (AML/CFT) regime to the financial system, financial industry as well as other socio-economic impacts in general.

C. Risk Assessment Stages and Risk Factors

Based on the FATF guidelines, there are three main stages involved in the risk assessment process as follows:

1. The **Identification** process identifies the threats, vulnerabilities and consequences. Ideally, at this stage, the identification process should attempt to be comprehensive. However, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.

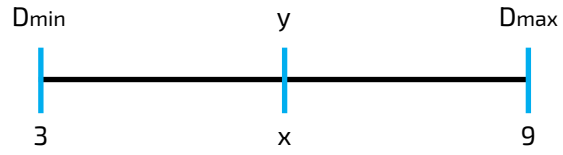
2. **Analysis** lies at the heart of the money laundering and terrorist financing risk assessment process. The goal of this stage is to analyse the identified risks in terms of their nature, sources, likelihood and consequences in order to understand each risk holistically as a function of threat, vulnerability and consequence.

Table 1.3. Matrix of Risk Factors in Non-Bank Payment Service Providers and Non-Bank Money Changers

Non-Bank Payment Service Providers and Non-Bank Money Changers
THREATS
Threat Risk Analysis
• Number of Suspicious Transaction Reports (STRs) relating to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. • Number of Suspicious Transaction Reports based on Cash Transaction Reports relating to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. • Number of court verdicts relating to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. • Emerging threats (perception and input from experts, supervisors and industry actors)
VULNERABILITIES
Vulnerability Risk Analysis
• Effectiveness of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction implementation by service provider • Ability to mitigate various risks associated with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction • Potential vulnerabilities (perception of supervisors and industry players)
CONSEQUENCES
Consequence Risk Analysis
• The value of suspicious transactions based on the Suspicious Transaction Report (STR) relating to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. • The suspicious transactions based on Cash Transaction Reports relating to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. • Value of transactions in terms of court verdicts • Potential Consequences (perception, inputs from experts, supervisors and industry actors)

Each key risk factor is converted to a scale of 3-9, where the data with the lowest value scores a 3 and the highest a 9. Intermediate values are commensurate with the value of the data. Data is transformed onto the scale using a simple mathematical equation as follows:

Figure 1.8. Data Conversion Formula for 3-9 Scale



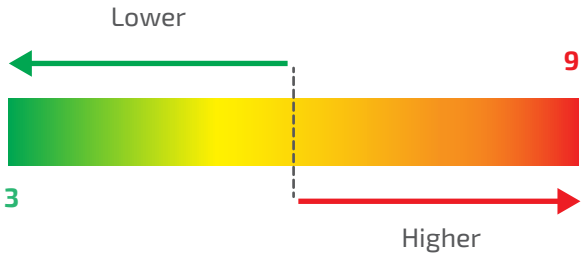
$$x = \frac{6\,(y - D_{min}) + 3}{D_{max} - D_{min}}$$

Source: NRA of Money Laundering and Terrorist Financing 2021

For each key risk, the respective risk factors are multiplied and averaged, producing a score on a scale of 3 - 9 for each threat, vulnerability and consequence. In accordance with the risk assessment framework, after calculating the value of threats and vulnerabilities, the two are added together to obtain the likelihood value. The likelihood value for each key risk is averaged and converted to a scale of 3-9.

The likelihood value is subsequently multiplied by the consequence scale to calculate the risk value. The scaled values of likelihood and consequence range between 3 and 9, therefore the smallest risk value is 9 (3x3) and 81 the largest (9x9). The risk values are converted to a scale of 3-9 by calculating the square root of each value.

Figure 1.9. Scale of Threats, Vulnerabilities and Consequences



Source: NRA of Money Laundering and Terrorist Financing 2021

The risk scores are divided into three categories, including low, medium and high based on a scale of 3-9.

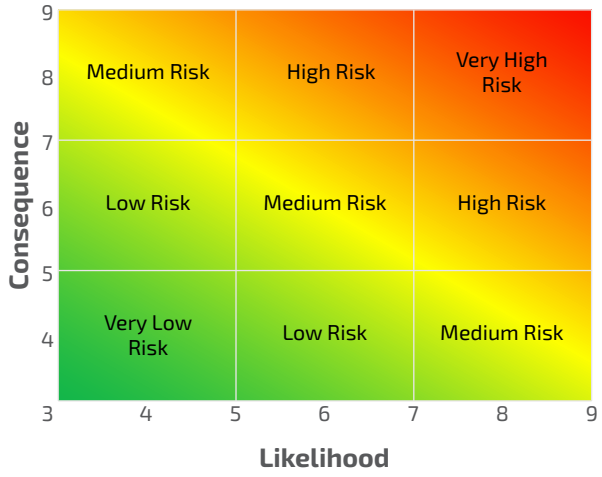
Table 1.4. Risk Scores

Risk Value Range	3 ≤ x < 5	5 ≤ x < 7	7 < x ≤ 9
Risk Score	Low	Medium	High

Source: NRA of Money Laundering and Terrorist Financing 2021

Each key risk is plotted on a risk matrix to facilitate comparison between the values of risk, likelihood and consequence, where the x-axis represents the likelihood and the y-axis the consequence.

Figure 1.10. Risk Analysis Matrix

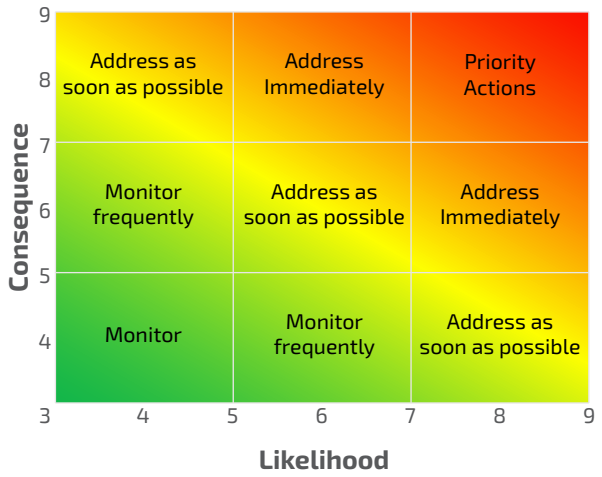


Source: NRA of Money Laundering and Terrorist Financing 2021

3. **Evaluation** in the context of money laundering and terrorist financing risk assessment process involves taking the risks analysed during the previous stage to determine priority actions for addressing them. Depending on the source, there are a number of methods for addressing (or controlling) risk, including prevention (or avoidance), mitigation (or reduction), acceptance or contingency planning.

The risk evaluation matrix for money laundering is as follows:

Figure 1.11. Risk Evaluation Matrix



Source: NRA of Money Laundering and Terrorist Financing 2021

D. Data Sources and Data Collection Techniques

Quantitative and qualitative data from various sources during the 2019-2020 period were used in this Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of proliferation of Weapons of Mass Destruction.

The following data and information were used to prepare the Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021:

1. Suspicious Transaction Reports (STR)
2. Cash Transaction Reports (CTR)
3. Court Reports on Money Laundering and Terrorist Financing
4. Risk Assessment Surveys performed in 2021 by non-bank payment service providers and non-bank money changers
5. Risk Assessment Surveys in 2021 performed by law enforcement agencies
6. Research on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction typologies
7. Outcome of the Indonesia Mutual Evaluation Report (MER)
8. Other literature studies

The data collection method used when preparing the SRA combined quantitative and qualitative approaches based on the following data collection techniques:

1. **Surveys and/or in-depth interviews** based on questionnaires prepared by Bank Indonesia and distributed to service providers and supervisors to identify and analyse the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, and to formulate mitigation measures for the key risks.

2. **Secondary data analysis** of statistical data collected from suspicious transaction reports, typologies and court reports regarding cases of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction sourced from the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

3. **Focus group discussions/working groups** with service providers and supervisors to identify and analyse the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, and to formulate mitigation measures for the key risks. Focus Group Discussions (FGD) and working groups were also organised with relevant government ministries/agencies, including the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) and law enforcement agencies to share information concerning the typologies and court verdicts regarding cases of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

4. **Comparative studies** to ascertain the typologies of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction cases as well as the risk mitigation measures taken in other countries.

5. **Discussions with related work units** to collect other information required to prepare the SRA 2021 as well as confirm the outcome of the latest SRA.

E. Stages of Risk Assessment

The process of risk assessment concerning money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank payment service providers and non-bank money changers in 2021 is as follows:

1. **Data Collection**

   During this stage, Bank Indonesia dispatched questionnaires on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction to Reporting Parties to assess the identification, detection and prevention measures implemented by the Reporting Parties. The survey was conducted in September 2021, involving approximately 183 non-bank money changers and 93 non-bank payment service providers.

2. **Discussion**

   Discussions were held with stakeholders to confirm the results of identification, analysis and evaluation in the risk assessment process. The discussion stage is also used to garner in-depth information from stakeholders, including in terms of determining the priority actions.

F. Research Limitations

The Sectoral Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction was compiled after completion of the National Risk Assessment. The limitations of the assessment are as follows:

1. The reporting parties as respondents in this research were located in medium- and high-risk regions, utilising a sample of large, medium and small reporting parties in each respective region.

2. Risk mapping of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the sectoral risk assessment comprised four key risks, namely Customer, Region, Product and Delivery Channel.

3. The sources of data used in the preparation of the sectoral risk assessment were survey data from service providers and supervisors, STR data and typology cases from the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), as well as court reports on cases of money laundering and terrorist financing from law enforcement agencies from 2019-2020.


Rp

PART II

NON-BANK MONEY CHANGERS

EXECUTIVE SUMMARY

In 2021, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), in conjunction with relevant government ministries/ agencies, identified, analysed and evaluated the latest money laundering risks holistically through the national risk assessment program, namely the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021. As a follow-up action to mitigate the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank money changers, a sectoral risk assessment (SRA) was performed with the following objectives:

1. Identifying and analysing the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank money changers;

2. Identifying, analysing and evaluating various risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction based on risk mapping the **Customers (individual and corporate), regions, products and services as well as delivery channels** in non-bank money changers;

3. Identifying and analysing the emerging threats of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank money changers.

4. Formulating strategic risk mitigation measures against money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank money changers.

The SRA of non-bank money changers mapped four key risks based on customer profile, region, product and service as well as delivery channel and formulated risk factors covering the threats, vulnerabilities and consequences. The analysis methodology referred to the risk assessment method published by the Financial Action Task Force (FATF). According to the latest assessment, the level of money laundering risk in non-bank money changers is as follows:

1. The **Special Capital Region of Jakarta** and province of **Riau Islands** are **high-risk** regions for money laundering activity in non-bank money changers, followed by the provinces of **West Java, Banten, East Java** and **North Sumatra** as **medium-risk** regions. All other provinces are **low** risk.

2. **Politically Exposed Persons (PEP), Private Sector Employees** and **Entrepreneurs** are **high-risk** individual customer profiles concerning money laundering activity in non-bank money changers, followed **Money Changer Employees** as **medium** risk. All other individual customers are **low** risk.

3. **Non-MSME Limited Liability Companies (PT) and Limited Partnership Companies (CV)** are **high-risk** institutional customer profiles for money laundering activity in non-bank money changers, followed by **Government Institutions** as **medium** risk. All other institutional customer profiles are **low** risk.

4. **USD and SGD** are **high-risk** products (foreign banknotes) for money laundering activity in non-bank money changers, followed by **EUR, AUD** and **MYR** as **medium** risk. All other foreign banknotes are **low** risk.

5. **Non-bank Money Changer Offices** are a **medium**-**risk** delivery channel for money laundering activity in non-bank money changers, with all other delivery channels considered **low** risk.

Based on the latest assessment, the level of terrorist financing risk in non-bank money changers is as follows:

1. The **Special Capital Region of Jakarta** is a **high-risk** region for terrorist financing activity in non-bank money changers, followed by the provinces of **East Java** and **Papua** as **medium**-**risk** regions. All other provinces are **low** risk.

2. **Private Sector Employees** and **Entrepreneurs** are **high-risk** individual customer profiles for terrorist financing activity in non-bank money changers, followed **Housewives** as **medium** risk. All other individual customer profiles are **low** risk.

3. **USD** is a **high-risk** product (foreign banknote) for terrorist financing activity in non-bank money changers, followed by **SGD** as **medium** risk. All other foreign banknotes are **low** risk.

4. **Non-Bank Money Changer Offices** are a **medium**-**risk** delivery channel for terrorist financing activity in non-bank money changers, with all other delivery channels considered **low** risk.

Seeking to mitigate the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank money changers, Bank Indonesia has issued regulations and guidelines, while implementing oversight and indirect supervision. In conjunction with the Indonesian National Police, Bank Indonesia has shut down unlicensed non-bank money changers throughout Indonesia. In addition, Bank Indonesia has also provided socialisation and education activities targeting non-bank money changers and members of the public to increase awareness of the risks and support efforts to prevent and eradicate money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

1

LITERATURE REVIEW OF NON-BANK MONEY CHANGERS

A. Legal Basis

Legally, Bank Indonesia is a supervisory and regulatory body (LPP) for non-bank money changers in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (ML Act). Provisions regarding non-bank money changers are stipulated in Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers and Bank Indonesia Circular Letter (SEBI) No. 18/42/DKSP, dated 30th December 2016, concerning Non-Bank Money Changers. The salient provisions of the Bank Indonesia Regulation on Non-Bank Money Changers are as follows:

1. Scope of business activity
2. Underlying transaction obligations
3. Licensing procedures and requirements
4. Governance and consumer protection
5. Buying and selling of foreign banknotes by third parties

B. Characteristics of Non-Bank Money Changers in Indonesia

1. Definition

Non-Bank Money Changers are non-bank business entities incorporated as a Limited Liability Company that exchange foreign currencies.[23] The business activities of non-bank money changers include buying and selling foreign banknotes[24] as well as purchasing traveller's cheques. In addition, non-bank money changers may engage in other business activities as regulated by prevailing Bank Indonesia regulations[25], such as carrying foreign banknotes.

A limited liability company operating as a non-bank money changer is required to first obtain a licence from Bank Indonesia. Licences for non-bank money changers issued by Bank Indonesia are valid for five years from the date of the licence and can be extended based on an application submitted by the non-bank money changer to Bank Indonesia. Licensed non-bank money changers are obliged to display:

a. The logo of licensed non-bank money changers issued by Bank Indonesia.
b. The licence certificate issued by Bank Indonesia.
c. An 'Authorised Money Changer' sign along with the name of the limited liability non-bank money changer displayed prominently at the business location.

Non-bank money changers are prohibited from:

a. Acting as a selling agent for traveller's cheques.
b. Performing margin trading, spot, forward, swap or other derivative transactions on behalf of a customer or the business itself.

23 Article 1, Paragraph 5 of Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers.

24 Article 1, Point 1 of Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers states that *Uang Kertas Asing* (UKA) are foreign banknotes issued by a competent authority outside of Indonesia and recognised as legal tender in the issuing country.

25 Article 2, Paragraph 2 of Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers.

c. Buying or selling foreign banknotes or purchasing traveller's cheques in conjunction with unlicensed non-bank money changers.

d. Performing money transfer services.

e. Performing other business activities.

In addition, the directors, commissioners and/or shareholders of non-bank money changers are prohibited from:

a. Owning unlicensed non-bank money changers.

b. Collaborating with unlicensed non-bank money changers.

c. Performing business activity through unlicensed non-bank money changers.

2. Products and Services

The business activities of non-bank money changers are as follows:

a. Exchange activity by purchasing and selling foreign banknotes.

b. Purchasing traveller's cheques.

The purchasing and selling mechanism for foreign banknotes is as follows:

a. Foreign banknotes must be handed over in person.

b. Rupiah banknotes must be handed over in person or via an intrabank or interbank transfer.

c. Purchases of foreign banknotes by a customer of a non-bank money changer that exceed a specific threshold[26] per month per customer must use an underlying transaction.

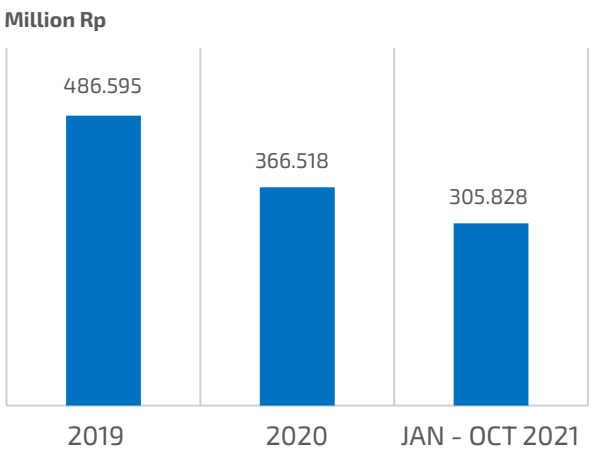
d. If foreign banknotes are purchased by a non-bank money changer, the obligations referenced in letter c are not applicable.

The products and services of non-bank money changers are foreign banknotes and purchasing traveller's cheques. Nationally, the purchase and sale of foreign banknotes fell significantly by 24.7% (yoy) in 2020 as a corollary of the Covid-19 pandemic. As of October 2021, transactions by non-bank money changers fell another 16.6% compared with conditions in 2020. The composition of most transacted foreign banknotes in 2021 was dominated by SGD (50%), followed by USD (33%) CNY (6%), MYR (3%) and THB (2%), thus indicating a shift from USD dominance in 2020.

3. Delivery Channels

As stipulated in the Bank Indonesia Regulation (PBI) concerning Non-Bank Money Changers, in terms of the purchasing and selling mechanism for foreign banknotes, all foreign banknotes must be surrendered in person, while rupiah banknotes can be handed over in person or via intrabank or interbank transfer. Considering that foreign banknotes must be handed over in person, transactions at non-bank money changers currently apply two mechanisms, namely direct transactions at the office of a non-bank money changer as well as foreign banknote delivery services.

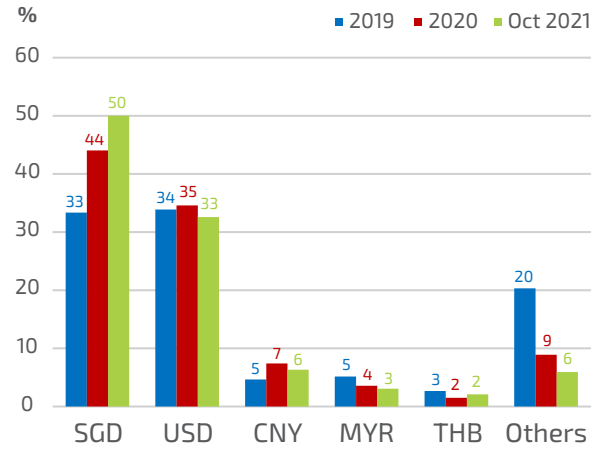
Graph 2.1. National Foreign Banknote Transactions by Non-Bank Money Changers



Source: Bank Indonesia

26 The threshold for purchasing foreign banknotes by customers of non-bank money changers refers to prevailing Bank Indonesia regulations concerning foreign exchange transactions against the rupiah between banks and domestic parties as well as Bank Indonesia regulations on foreign exchange transactions against the rupiah between banks and foreign parties. Currently, the threshold is set at USD25,000 or equivalent in accordance with Bank Indonesia Regulation (PBI) No. 18/19/PBI/2016.

Graph 2.2. Composition of Foreign Banknote Transactions at Non-Bank Money Changers by Currency



Source: Bank Indonesia

4. Regional Distribution

The number of licensed non-bank money changers in Indonesia is growing annually. Based on distribution data, non-bank money changers are concentrated in Jakarta, Riau Islands, Bali, East Java and West Java. The distribution of non-bank money changers in Indonesia is recapitulated as follows:

Table 2.1. Distribution of Non-Bank Money Changers as of December 2021

No	Province	Total
1	Special Capital Region of Jakarta	298
2	Bali	127
3	Riau Islands	115
4	East Java	102
5	West Java	64
6	Banten	51
7	North Sumatra	49
8	Central Java	36
9	West Kalimantan	22
10	West Nusa Tenggara	19
11	Aceh	16
12	West Sumatra	14
13	Riau	14
14	Special Region of Yogyakarta	13
15	South Sumatra	8
16	East Nusa Tenggara	6
17	South Sulawesi	4
18	Lampung	4
19	North Sulawesi	3
20	Papua	3
21	West Papua	2
22	Jambi	2
23	North Maluku	1
24	Bengkulu	1
25	North Kalimantan	1
26	South Kalimantan	1
27	East Kalimantan	1
	Total	**977**

Source: Bank Indonesia

2

KEY RISKS IN NON-BANK MONEY CHANGERS

A. Money Laundering Risk Landscape

The typologies of money laundering have evolved in Indonesia to become more complex and varied over time. Money laundering can exploit financial institutions and non-financial institutions. Based on the National Risk Assessment (NRA) of Money Laundering, cases in Indonesia are dominated by the predicate offences of narcotics and corruption. Perpetrators also exploit automotive dealerships, estate agents, commercial banks and non-bank money changers to conceal their financial activity. Meanwhile, most money laundering criminals are employed as government/legislative officials or employees of state/regional-owned enterprises, or business entities incorporated as limited liability companies. The highest risk region for money laundering is Jakarta, with the typologies dominated by use of false identification, nominees, trusts, family members or third parties, estate agents, smurfing[27], structuring[28], using professional services, using new payment methods/systems, using legal persons and exploiting unregulated sectors.

Furthermore, mapping the foreign inward risk or Foreign Predicate Crime (FPC)[29] based on the NRA showed that fraud, corruption, money transfers, narcotics, electronic information and transactions (EIT) or cybercrime are the highest risk predicate offences of money laundering in Indonesia. Meanwhile, the highest risk countries of origin in terms of predicate crimes are Malaysia, Japan, Singapore, Thailand, Saudi Arabia and the United Arab Emirates. Based on individual customer profile, entrepreneurs, private sector employees, merchants, housewives, professionals and consultants, students, civil servants (including retirees) as well as lecturers/professors are high risk. In terms of business segment, industry and distribution were shown to be high-risk categories for foreign predicate crimes (FPC).

Mapping the foreign outward risk or laundering offshore (LO) revealed that corruption and narcotics are high-risk foreign predicate crimes. High-risk destination countries for laundering offshore include Singapore, United States, India, China, Thailand, Malaysia and Hong Kong. Based on individual customer profile, government/legislative officials, entrepreneurs and private sector employees are high-risk for laundering offshore. In terms of business segment, industry is a high-risk category for laundering offshore.

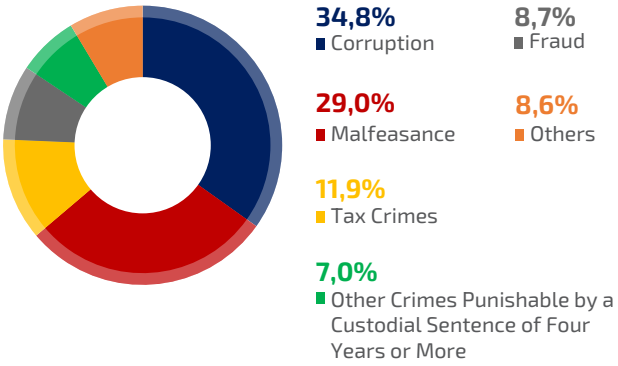
Data from the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) shows that several predicate offences tend to exploit non-bank money changers, including corruption, malfeasance, tax crimes, fraud, banking crimes and other crimes punishable by a custodial sentence of four years or more.

27 Smurfing is a money-laundering technique involving the use of several different accounts on behalf of one customer.

28 Structuring is a money-laundering technique using relatively small, yet high-frequency, transactions in the financial sector.

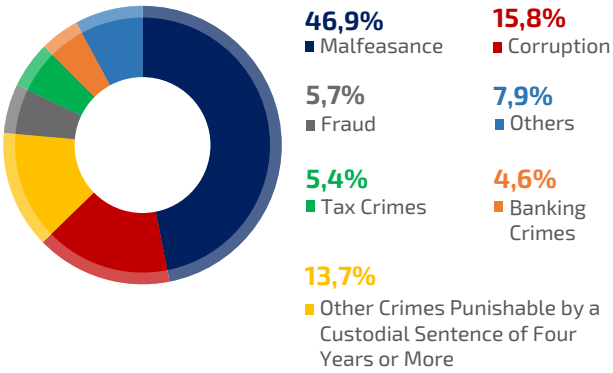
29 Foreign inward risk or foreign predicate crime is money laundering in Indonesia with the predicate offences perpetrated abroad.

Graph 2.3. Composition of Predicate Crimes of Money Laundering in Non-Bank Money Changers based on Suspicious Transaction Value



Source: Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)

Graph2.4. Composition of Predicate Crimes of Money Laundering in Non-Bank Money Changers based on Total Suspicious Transaction Reports



Source: Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)

According to Money Laundering through Money Remittance and Currency Exchange Providers published by the Financial Action Task Force (FATF) in 2010, several factors have been identified that leave non-bank money changers vulnerable to exploitation by money launderers, including small denominations and straightforward buying-selling transactions, widespread use of cash and the dominance of walk-in customers that exposes vulnerabilities in the customer identification and verification process. In addition, foreign banknote buying-selling transactions that facilitate the transfer of rupiah to and from third parties can obscure the actual beneficial parties involved in the transaction. Several typologies of money laundering using non-bank money changers have been identified as follows:

1. Purchasing foreign banknotes by parties other than the beneficial owner.
2. Transferring rupiah banknotes but collecting foreign banknotes in cash by a different person.
3. Surrendering foreign banknotes in person but transferring rupiah to a separate account or several accounts.
4. Transferring rupiah banknotes to several accounts owned by one individual or beneficial owner (smurfing). The accounts typically use nominees, trustees, family members or third parties.
5. Transactions not in accordance with the customer profile.
6. Large purchases of foreign banknotes in cash where the customer cannot or refuses to provide information on the source of funding.
7. Significant foreign currency exchange transactions involving different currencies in one transaction.
8. Significant foreign currency exchange transactions by Politically Exposed Persons (PEP).
9. Significant transactions without clear underlying transactions.
10. Use of individual/personal accounts for the operating activities of non-bank money changers as a media/vehicle for the illicit proceeds of crime.
11. Use of unlicensed non-bank money changers.
12. Use of false identification documents when exchanging foreign currencies.
13. Exchanging large-denomination foreign banknotes, such as the SGD10,000 banknote.
14. Transactions not recorded in the non-bank money changer's system and without providing a receipt.

15. High-frequency transactions of relatively small value during a given period (structuring). Transactions using more than one non-bank money changer within a brief period.

16. Trade-based money laundering, transfer pricing and use of shell companies to produce fictitious invoices used as underlying transactions for foreign currency exchange transactions at non-bank money changers.

17. Exchanging significant amounts of small-denomination banknotes for large-denomination banknotes.

18. Exchanging significant amounts of uncommon foreign banknotes.

Examples of money laundering cases involving non-bank money changers are as follows:

Criminal case against DY (Jakarta High Court Case Number: 57/PID.SUS/2019/PT.DKI) for money laundering with the predicate offence of narcotics and the following typology:

a. The defendant owned six fictitious companies, including trading, supplier and investment companies but the only business activity was exchanging foreign currencies, similar to a non-bank money changer. The defendant exploited the trading and supplier companies as importers of foreign goods by falsifying invoices to make payments abroad with transactions to several countries, including China, India, Japan, Germany and Australia. There were also indications of a link between the money laundering case and online gambling activities involving DY and the non-bank money changer business.

b. DY ran an unlicensed non-bank money changer and used several bank accounts in the names of employees to receive money transfers from narcotics networks to conceal the activity from law enforcement agencies.

Criminal case against NL (Tangerang High Court Case Number: 318/Pid.Sus/2019/Pn.Tng) for money laundering with the predicate offence of narcotics and using an licensed non-bank money changer with the following typology:

a. The defendant was employed by the family business, a licensed non-bank money changer, which was used to receive and transfer proceeds from narcotics crimes.

b. The defendant set up several shell companies, with the corporate accounts used to transfer funds. The defendant used accounts belonging to himself, others and the businesses to transfer funds between accounts to conceal financial activity. The defendant also acted on behalf of other people concerning the proceeds of narcotics crime.

c. The proceeds of crime were stored in an account belonging to the non-bank money changer, the defendant and other people, and used to buy and sell foreign exchange, thereby mingling[30] the illicit funds with legal business activity.

B. Terrorist Financing Risk Landscape

In the context of terrorist financing and financing of proliferation of weapons of mass destruction in Indonesia, the typologies are becoming more complex and varied, exploiting financial institutions and non-financial institutions.

Based on the National Risk Association (NRA) of Terrorist Financing 2021, funds used for financing domestic terrorist activities derived from within the country or abroad as well as funds derived from within Indonesia for foreign terrorist activity

30 Mingling is a money-laundering technique involving the consolidation of illegal funds in legal business activities.

are considered high threats. In terms of the typologies, fundraising by terrorist financiers and funds embezzled from donations through community organisations are considered high risk for terrorist activity. In terms of transferring funds, most use financial service providers, specifically banks, money or value transfer service providers, and money changers. Terrorist funds are also at high risk of being used to purchase arms and explosives, training in the manufacture of arms and explosives as well as travel expenses to and from domestic terrorist operations. Based on individual customer profile, those most at risk of funding terrorists include entrepreneurs, while institutional customers include limited liability companies (PT), foundations, associations and limited partnership companies (CV). Meanwhile, the highest risk regions were Jakarta, East Java, West Java and Central Java.

Furthermore, the results of mapping foreign inward risk or foreign predicate crime (FPC) based on the NRA showed that the high-risk sources of terrorist financing into Indonesia are the United States, Malaysia, the Philippines and Australia. Meanwhile, mapping the foreign outward risk or laundering offshore (LO) showed that the high-risk destinations for LO include Malaysia, the Philippines and Australia. In addition, there are several emerging threats concerning terrorist financing that must be mitigated moving forward as follows:

1. Terrorist financing by corporate (institutional) sponsors.
2. Narco-terrorism.
3. Use of virtual currency for terrorist financing.
4. Use of online/peer-to-peer lending for terrorist financing.
5. Activities of armed criminal groups in the country.

Terrorist financing using non-bank money changers aims to convert foreign currencies into rupiah, or vice versa, to facilitate the financing of terrorist activities. According to data from the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), several terrorist financing typologies using non-bank money changers have been identified as follows:

1. Purchasing foreign banknotes by parties other than the beneficial owner.
2. Transactions not in accordance with the customer profile.
3. Relatively small, yet high-frequency, transactions (structuring).

C. Money Laundering Risk Assessment Analysis

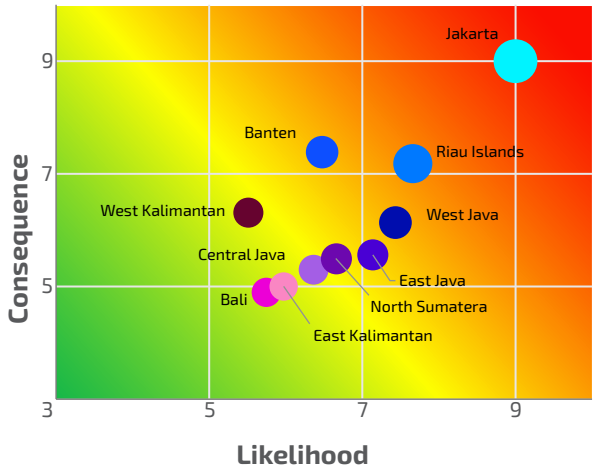
1. Money Laundering Risk by Region

A risk assessment of money laundering in the non-bank money changer sector was performed based on region to ascertain which provinces were at the highest risk of money laundering cases. The sectoral risk assessment by region measured the threats, vulnerabilities and consequences in each respective province based on predetermined risk factors.

Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability. The salient outcomes of the regional risk analysis of money laundering in the non-bank money changer sector are recapitulated in Table 2.2.

The results of mapping money laundering risk in the non-bank money changer sector by region is presented in Figure 2.1

Figure 2.1. ML Risk Heatmap by Region in Non-Bank Money Changer Sector



Based on the risk heatmap presented in Figure 2.1, the provinces with a high level of money laundering risk in non-bank money changers are **Jakarta** and **Riau Islands**, followed by **West Java, Banten, East Java** and **North Sumatra** as **medium**-risk regions. All other regions are **low** risk.

Jakarta and **Riau Islands** recorded the highest scores for risk compared to other regions, as reflected by the high frequency and value of suspicious transactions and cash transactions. Notwithstanding, the level of risk in Jakarta was significantly higher than Riau Islands in line with the court reports from 2019-2020, dominated by money laundering cases in Jakarta. The high-risk status of Riau Islands was confirmed by the outcome of a Sectoral Risk Assessment in 2017 targeting the Customs and Excise sector, stating that the Riau Islands are high risk for money laundering due to the geographical location of the region, namely its proximity to the border, thus providing high potential for money laundering, particularly through the carrying of cash across borders.

Table 2.2. Risk Analysis of Money Laundering in Non-Bank Money Changers by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Special Capital Region of Jakarta	9.00	9.00	9.00	9.00	**9.00**	High
2.	Riau Island	7.54	7.12	7.18	7.29	**7.98**	High
3.	West Java	6.91	7.98	6.13	7.42	**6.18**	Medium
4.	Banten	6.04	6.99	7.39	6.47	**5.90**	Medium
5.	East Java	6.16	8.17	5.56	7.14	**5.53**	Medium
6.	North Sumatra	5.82	7.47	5.53	6.61	**5.26**	Medium
7.	Others	3.90	5.79	4.09	4.78	**3.82**	Low

The provinces of **West Java, East Java** and **North Sumatra** are **medium**-risk regions due to the **medium** level of threat and consequence but a **high** level of vulnerability. Meanwhile, **Banten** is a **medium**-risk region due to the **medium** level of threat and vulnerability but **high** level of consequence. Medium threat and consequence scores are reflected in the high frequency and value of money laundering cases in the respective regions, though still below the levels recorded in Jakarta. The high vulnerability stemmed from suboptimal AML/CFT implementation in the respective regions, coupled with the perception of law enforcement agencies concerning the constraints to handling cases in regions where the offences occur. The large number of non-bank money changers operating in those areas also influenced the higher risk exposure to money laundering in those six regions.

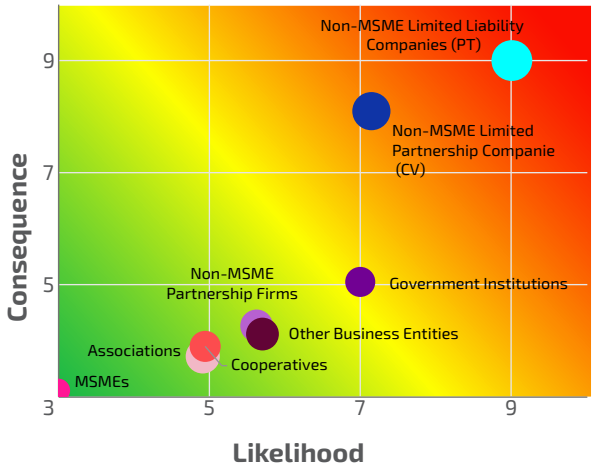
2. Money Laundering Risk by Corporate Customer Profile

According to money laundering risk analysis based on actors in the National Risk Assessment of Money Laundering 2021, Corporate and Individual customer profiles were shown to be high risk domestically. Therefore, a risk analysis of money laundering based on business entity was necessary to understand which types of corporate customer profile were most at risk of money laundering in the non-bank money changer sector.

The results of money laundering risk analysis in non-bank money changers based on corporate customer profile are presented in Table 2.3.

The results of mapping money laundering risk in the non-bank money changer sector by corporate customer profile are presented in Figure 2.2.

Figure 2.2. ML Risk Heatmap by Corporate Customer Profile in Non-Bank Money Changer Sector



According to the risk heatmap presented in Figure 2.2, **Non-MSME Limited Liability Companies (PT)** and **Non-MSME Limited Partnership Companies (CV)** are **high** risk for money laundering in the non-bank money changer sector, while **Government Institutions** are **medium** risk. All other business entities are **low** risk.

Non-MSME Limited Liability Companies (PT) and **Non-MSME Limited Partnership Companies (CV)** recorded the highest scores in terms of risk compared to other corporate customer profiles. This was reflected in court report data from 2019-2020, showing that both types of corporate customer profile dominated

Table 2.3. Risk Analysis of Money Laundering in Non-Bank Money Changers by Corporate Customer Profile

No	Customer Profile	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-MSME Limited Liability Companies (PT)	9.00	8.65	9.00	9.00	**9.00**	High
2.	Non-MSME Limited Partnership Companies (CV)	6.86	7.19	8.10	7.15	**7.07**	High
3.	Government Institutions	4.76	9.00	5.02	7.00	**5.16**	Medium
4.	Others	3.94	5.68	3.72	4.87	**3.77**	Low

money laundering cases. This is also in line with the outcome of the National Risk Assessment of Money Laundering 2021, confirming that Non-MSME Limited Liability Companies (PT) are high risk due to various money laundering cases involving such types of corporate customer profile. Meanwhile, **Government Institutions**, in this case state/regional-owned enterprises, are medium risk because of the perception of law enforcement agencies concerning the constraints to handling such cases and the expected consequence if such businesses were engaged in money laundering. This was reinforced by the perception of reporting parties and supervisors, stating that state/regional-owned enterprises are high risk in terms of money laundering.

Based on the National Risk Assessment of Money Laundering 2021, vulnerability due to a suboptimal identification and verification process concerning beneficial ownership, as well as the significant consequences for the financial system and economy if money laundering is committed by a business entity, implies that corporations are high risk if used as a medium for money laundering.

3. Money Laundering Risk based on Individual Customer Profile

Money laundering risk was also assessed based on individual customer profile to ascertain which professions are most at risk to committing money laundering via non-bank money changers.

The results of money laundering risk analysis in non-bank money changers based on individual customer profile are presented in Table 2.4.

The results of mapping money laundering risk in the non-bank money changer sector by individual customer profile is presented in Figure 2.3.

Gambar 2.3. ML Risk Heatmap by Individual Customer Profile in Non-Bank Money Changer Sector

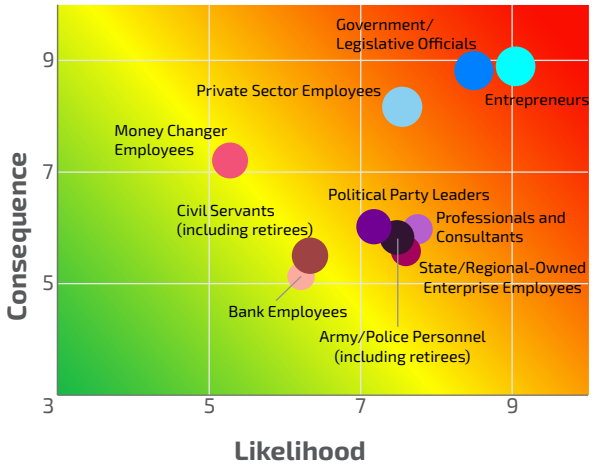


Table 2.4. Risk Analysis of Money Laundering in Non-Bank Money Changers by Individual Customer Profile

No	Profession	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Entrepreneurs	9.00	7.55	9.00	9.00	**9.00**	High
2.	Government/Legislative Officials	6.70	9.00	8.89	8.45	**8.51**	High
3.	Private Sector Employees	8.34	5.94	8.16	7.53	**7.37**	High
4.	Army/Police Personnel (including retirees)	6.69	7.51	5.80	7.48	**5.87**	Medium
5.	Political Party Leaders	5.24	8.49	6.02	7.18	**5.85**	Medium
6.	State/Regional-Owned Enterprise Employees	6.36	8.01	5.62	7.59	**5.80**	Medium
7.	Money Changer Employees	4.58	6.11	7.11	5.20	**5.33**	Medium
8.	Civil Servants (including retirees)	6.46	5.97	5.49	6.33	**5.15**	Medium
9.	Other Professions	4.31	5.57	4.34	5.33	**4.75**	Low

According to the risk heatmap presented in Figure 2.3, **Entrepreneurs, Government/ Legislative Officials** and **Private Sector Employees** are high risk for money laundering in the non-bank money changer sector, while **Political Party Leaders, Army/Police Personnel (including retirees), Money Changer Employees, Civil Servants (including retirees)** and **State/Regional-Owned Enterprise Employees (including retirees)** are **medium** risk customer profiles. All other customer profiles are **low** risk.

Entrepreneurs, Government/Legislative Officials and **Private Sector Employees** recorded the highest scores in terms of risks compared to other customer profiles due to strong indications of money laundering cases involving such customer profiles based on suspicious transaction reports and cash transaction reports in terms of frequency and value. In addition, court report data from 2019-2020 showed that **entrepreneurs** and **private sector employees** were most frequently involved in cases of money laundering using non-bank money changers. Based on an analysis of existing cases, **entrepreneurs** typically created shell companies operating as non-bank money changers, which were used to transfer the proceeds of money laundering.

Pursuant to Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Combating The Financing of Terrorism for Non-Bank Payment Service Providers and Non-Bank Money Changers, and referring to FATF Guidance on Politically Exposed Persons (PEP), customer profiles included in the category of Politically Exposed Persons are particularly vulnerable to money laundering. Therefore, prospective customers, customers and beneficial owners categorised as PEP are considered high risk. As reported in the National Risk Assessment of Money Laundering 2021, customer profiles categorised as Domestic PEP include **Government/Legislative Officials, State/ Regional Enterprise Employees (including retirees), Civil Servants (including retirees), Army/Police Personnel (including retirees),** Lecturers and Professors serving as University Rectors, as well as **Political Party Leaders**.

Money Changer Employees are medium risk for money laundering in the non-bank money changer sector. According to an analysis of cases based on court reports, a motive was established for money changer employees to exploit non-bank money changers to receive and transfer funds. In addition, the proceeds of money laundering are also consolidated with money from foreign exchange trading activities (mingling) to conceal the origin of the funds. Furthermore, the Professional Money Laundering publication issued by FATF in 2018 found that the international financial system facilitates large-scale professional money laundering (PML) schemes. Employees of financial institutions from the lowest to the highest echelons are significantly vulnerable as professional money launderers (PMLs).

In general, employees are involved in creating or receiving supporting documents for false transactions without adequate customer due diligence, monitoring the flows of money laundering proceeds as well as manipulating financial transactions to avoid reporting obligations concerning suspicious transactions. The FATF publication also revealed cases involving cross-border currency couriers as part of the professional money laundering network. In this case, money changer employees, which can act as couriers, are highly vulnerable as part of the professional money laundering network. Money Laundering through Money Remittance and Currency Exchange Providers, published by FATF in 2010, listed the following individual customer profiles and behaviours as potential indicators of high money laundering risk:

a. The customer requests currency in large denomination notes.

b. The customer buys currency that does not fit with what is known about the customer's destination.

c. The customer buys currency from an unusual location compared to his/her own location.

d. The customer apparently does not know the exact amount being exchanged.

e. The customer looks around all the time and does not watch the counting of money.

4. Money Laundering Risk based on Products and Services

Money laundering risk was also assessed based on products and services to ascertain which were most at risk to cases of money laundering in non-bank money changers. The products and services of non-bank money changers are foreign banknotes and purchasing traveller's cheques. In terms of foreign banknotes, the risk analysis focused on the **10 most traded currencies by non-bank money changers**. In addition, in accordance with Article 2 of Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers, foreign banknotes must be surrendered in person, while rupiah banknotes may be handed over in person or via interbank and intrabank transfer. Therefore, the buying and selling mechanism for foreign banknotes, namely rupiah transfers as well as handing over rupiah and foreign banknotes in cash, is also analysed in terms of risk based on products and services.

The results of money laundering risk analysis in non-bank money changers based on products and services using several risk factors in the form of risk are presented in Table 2.5.

The results of mapping money laundering risk in the non-bank money changer sector by product and service is presented in Figure 2.4.

According to the risk heatmap presented in Figure 2.4, **USD** and **SGD** are **high**-risk products for money laundering in the non-bank money changer sector, while **AUD, EUR** and **MYR** are **medium** risk.

Figure 2.4. ML Risk Heatmap by Product and Service in Non-Bank Money Changer Sector

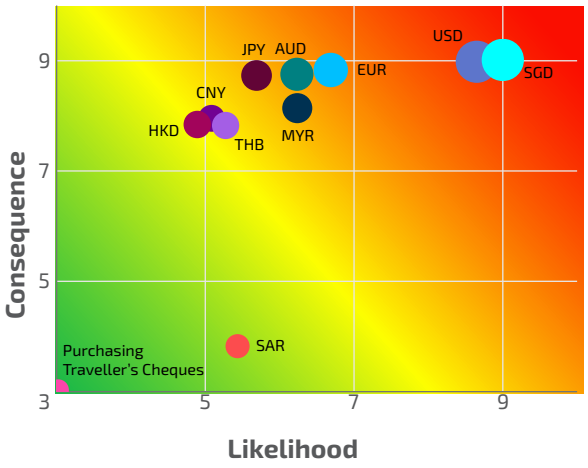


Table 2.5. Risk Analysis of Money Laundering in Non-Bank Money Changers by Product and Service

No	Product	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	SGD	8.67	9.00	9.00	9.00	9.00	High
2.	USD	9.00	7.99	8.98	8.65	8.99	High
3.	EUR	7.55	5.99	8.83	6.87	5.89	Medium
4.	AUD	6.66	5.99	8.75	6.42	5.19	Medium
5.	MYR	6.81	5.98	8.14	6.49	5.03	Medium
6.	Others	4.86	4.82	6.54	4.89	3.71	Low

USD and **SGD** products recorded the highest values of risk compared to the other products. The high frequency and value of suspicious transactions increased the level of threat and consequence for both products. In addition, court reports showed that USD and SGD were the most commonly used products for money laundering. Risk analysis by law enforcement agencies and reporting parties also confirmed a high level of risk for both products.

AUD, EUR and **MYR** are medium risk due to the relatively high number of suspicious transaction reports and court reports concerning those three products, yet still below USD and SGD.

Based on the buying and selling mechanism for foreign banknotes, transfers are higher risk than cash according to the analysis of court reports, showing that rupiah transfers were dominant in cases of money laundering. In addition, the current paradigm shift among members of the public from cash to cashless accelerated by the Covid-19 pandemic has increased the risk of using the transfer mechanism for money laundering purposes. Money Laundering through Money Remittance and Currency Exchange Providers, published by FATF in 2010, also confirmed that structuring and smurfing, which aim to break up transactions by transferring funds to various accounts, are the most common ML typologies found among non-bank money changers.

5. Money Laundering Risk based on Delivery Channel

Money laundering risk was also assessed based on the delivery channel to ascertain which delivery channels were most at risk to cases of money laundering in non-bank money changers. The delivery channels as objects of this risk assessment are grouped into two main categories, namely the offices of non-bank money changers and delivery services. With the development of digital technology, however, unlicensed non-bank money changers have been found buying and selling foreign banknotes via online merchants, thus necessitating a risk assessment of this new delivery channel.

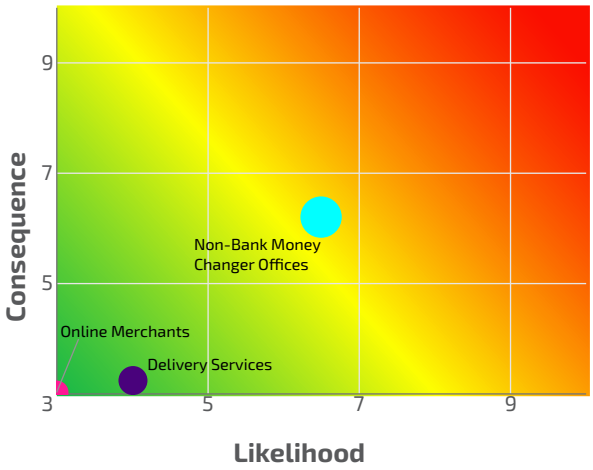
Using risk factors in the form of risk, the level of risk for each delivery channel in non-bank money changers was assessed and the results presented in Table 2.6.

Table 2.6. Risk Analysis of Money Laundering in Non-Bank Money Changers by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-Bank Money Changer Offices	6.60	6.74	6.60	6.74	**6.74**	Medium
2.	Delivery Services	4.14	4.76	3.27	4.11	**4.25**	Low
3.	Online Merchants	3.00	4.58	3.00	3.00	**3.00**	Low

The results of mapping money laundering risk in the non-bank money changer sector by delivery channel is presented in Figure 2.5.

Figure 2.5. ML Risk Heatmap by Delivery Channel in Non-Bank Money Changer Sector



According to the risk heatmap presented in Figure 2.5, **Non-Bank Money Changer Offices** are a **medium-risk** delivery channel for money laundering in the non-bank money changer sector, while other delivery channels are **low** risk.

Non-Bank Money Changer Offices recorded the highest risk scores compared to other delivery channels. Court reports from 2019-2020 showed that non-bank money changer offices were the delivery channel invariably used for money laundering purposes. This was confirmed by the results of a risk assessment by law enforcement agencies, which showed a high vulnerability in that delivery channel.

Delivery Services are low risk but the results of a risk assessment by law enforcement agencies showed a higher level of vulnerability in the delivery services channel. The reporting parties also found that Delivery Services are high risk in terms of money laundering. Meanwhile, **Online Merchants** are **low** risk but a risk assessment by reporting parties categorised this delivery channel as medium risk.

D. Terrorist Financing Risk Assessment Analysis

1. Risk Analysis by Region

Terrorist financing risk in non-bank money changers was assessed by region to find out which regions (provinces) were at risk of terrorist financing. The risk analysis by region was performed based on the level of risk in each respective province, measured in accordance with the predetermined risk factors.

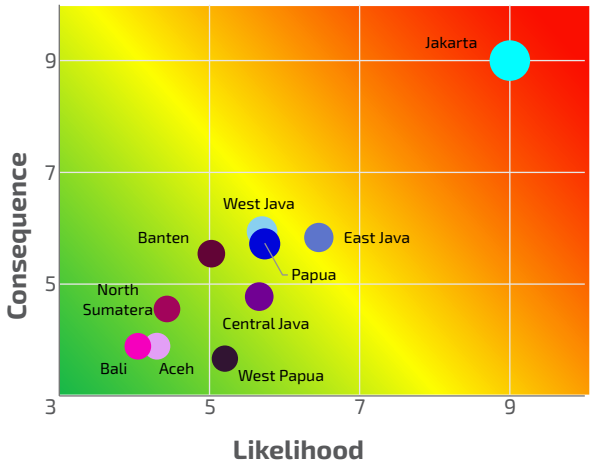
Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability scores. The salient outcomes of the regional risk analysis of terrorist financing in the non-bank money changer sector are recapitulated in Table 2.7.

Table 2.7. Risk Analysis of Terrorist Financing in Non-Bank Money Changers by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Special Capital Region of Jakarta	9.00	9.00	9.00	9.00	9.00	High
2.	East Java	4.88	8.08	5.83	6.46	5.47	Medium
3.	Papua	3.63	7.98	5.67	5.78	5.46	Medium
4.	Others	3.89	4.66	4.05	4.24	3.86	Low

The results of mapping terrorist financing risk in the non-bank money changer sector by region is presented in Figure 2.6

Figure 2.6. TF Risk Heatmap by Region in Non-Bank Money Changer Sector



Based on the risk heatmap presented in Figure 2.6, **Jakarta** is the only province with a **high** risk of terrorist financing in non-bank money changers, followed by **East Java** and **Papua** as **medium**-risk regions. All other regions are **low** risk.

Jakarta recorded the highest values of risk compared with other regions, as reflected in the suspicious transaction reports and cash transaction reports as well as court reports from 2019-2020.

The provinces of **East Java** and **Papua** are **medium**-risk regions due to the high level of vulnerability based on risk assessments conducted by law enforcement agencies and reporting parties. Meanwhile, East Java scored a medium level of consequence based on the value of terrorist financing cases in the region, albeit lower than Jakarta.

2. Terrorist Financing Risk based on Individual Customer Profile

Terrorist financing risk was also assessed based on individual customer profile to ascertain which professions were most at risk to terrorist financing via non-bank money changers.

The results of terrorist financing risk analysis in non-bank money changers based on individual customer profile are presented in Table 2.8.

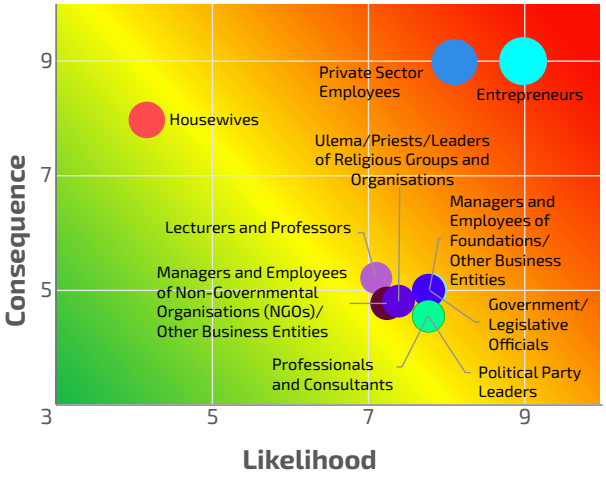
The results of mapping terrorist financing risk in the non-bank money changer sector by individual customer profile is presented in Figure 2.7.

According to the TF risk heatmap presented in Figure 2.7, **Entrepreneurs** and **Private Sector Employees** are **high** risk of terrorist financing in the non-bank money changer sector, while **Housewives** are **medium** risk customer profiles. All other customer profiles are **low** risk.

Table 2.8. Risk Analysis of Terrorist Financing in Non-Bank Money Changers by Individual Customer Profile

No	Profession	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Private Sector Employees	9.00	5.04	8.98	8.10	**9.00**	High
2.	Entrepreneurs	8.71	6.69	9.00	8.98	**8.46**	High
3.	Housewives	4.50	3.00	7.72	3.84	**6.38**	Medium
4.	Other Professions	4.55	6.26	4.58	4.99	**4.72**	Low

Figure 2.7. TF Risk Heatmap by Individual Customer Profile in Non-Bank Money Changer Sector



Entrepreneurs and **Private Sector Employees** recorded high scores in terms of threat and consequence, and a medium level of vulnerability due to strong indications of terrorist financing cases involving such customer profiles based on suspicious transaction reports and cash transaction reports in terms of frequency and value. The results of risk assessments conducted by supervisors also confirmed the high-risk status of both customer profiles.

Meanwhile, **Housewives** are medium-risk customer profiles based on suspicious transaction reports and cash transaction reports, though not as high as Entrepreneurs and Private Sector Employees. The results of risk assessments conducted by supervisors also confirmed the medium-risk status of housewives.

The results of terrorist financing risk analysis in non-bank money changers based on individual customer profile are also consistent with the National Risk Assessment of Terrorist Financing 2021, revealing that Entrepreneurs are high risk for terrorist financing, while Private Sector Employees and Housewives are medium risk. Based on the Sectoral Risk Assessment survey of reporting parties, 72% of non-bank money changer customers are dominated by Private Sector Employees (47%), Entrepreneurs (16%) and Housewives (10%). Such conditions create a potentially higher risk of non-bank money changers being exploited for terrorist financing by those customer profiles.

3. Terrorist Financing Risk based on Products and Services

Terrorist financing risk was also assessed based on products and services to ascertain which posed the most risk to cases of terrorist financing in non-bank money changers. The products and services of non-bank money changers are foreign banknotes and purchasing traveller's cheques. In terms of foreign banknotes, the risk analysis focused on the **10 most traded currencies by non-bank money changers**. In addition, in accordance with Article 2 of Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers, foreign banknotes must be surrendered in person while rupiah banknotes may be handed over in person or via interbank and intrabank transfer. Therefore, the buying and selling mechanism for foreign banknotes, namely rupiah transfers as well as surrendering rupiah and foreign banknotes in cash, is also analysed in terms of risk based on products and services.

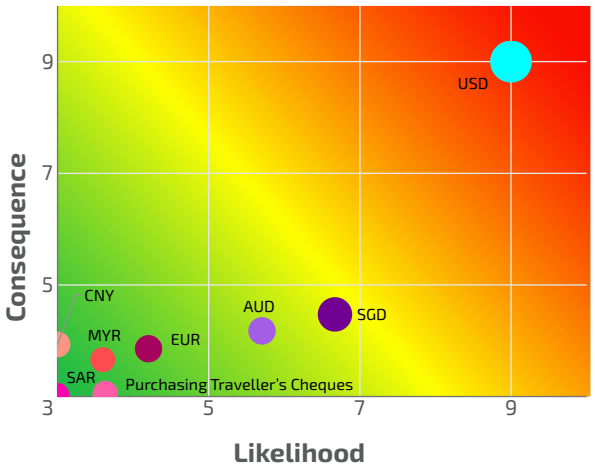
The results of terrorist financing risk analysis in non-bank money changers based on products and services using several risk factors in the form of risk are presented in Table 2.9.

Table 2.9. Risk Analysis of Terrorist Financing in Non-Bank Money Changers by Product and Service

No	Product	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	USD	9.00	9.00	9.00	9.00	9.00	High
2.	SGD	6.01	5.39	4.24	6.24	6.38	Medium
3.	Others	3.39	3.94	3.41	3.64	3.54	Low

The results of mapping terrorist financing risk in the non-bank money changer sector by product and service is presented in Figure 2.8.

Figure 2.8. TF Risk Heatmap by Product and Service in Non-Bank Money Changer Sector



According to the TF risk heatmap presented in Figure 2.8, **USD** is considered a **high**-risk product for terrorist financing in the non-bank money changer sector, while **SGD** is a **medium**-risk product. All other foreign currencies are **low** risk.

USD recorded the highest values of risk compared to the other products, as reflected in the high frequency and value of suspicious transactions involving USD. One court case showed that a perpetrator of terrorist financing was identified exchanging USD via non-bank money changers. The perpetrator targeted small non-bank money changers to exploit gaps in effective AML/CFT implementation. Risk analysis by law enforcement agencies and reporting parties also confirmed a high level of risk for USD in terms of terrorist financing. USD is readily available and widely accepted in many countries where terrorist acts are perpetrated, making it easier for terrorists to use and circulate USD but harder to track and control on the prevention side.

SGD is a medium-risk product, receiving medium scores in terms of threat and vulnerability but a low consequence level. Suspicious transaction reports involving SGD were discovered but at a lower rate than USD. In addition, the value of SGD transactions is lower than USD, creating a smaller potential impact or consequence.

Based on the buying and selling mechanism for foreign banknotes, cash is higher risk based on the high threat and vulnerability scores according to the high number of suspicious transaction reports. Moreover, court reports show that perpetrators of terrorist financing were requested to collect and hand over foreign banknotes in cash through non-bank money changers. The outcome of the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021 also confirmed the risk of terrorist financing through cash transactions by terrorist groups due to the simplicity, convenience and lack of traceability. Banknotes can be broken down into smaller denominations and smaller value transactions, thus making it easier for couriers (mules) to smuggle the banknotes across certain border crossings that are not well supervised according to law enforcement agencies.

Despite the lower risk of terrorist financing, transfers also pose a potential terrorist financing risk though non-bank money changers, particularly using nominees, family members and other accounts to obstruct the

identification and tracking process. Buying and selling as well as using third-party accounts also facilitate terrorist financing via the transfer mechanism.

4. Terrorist Financing Risk based on Delivery Channel

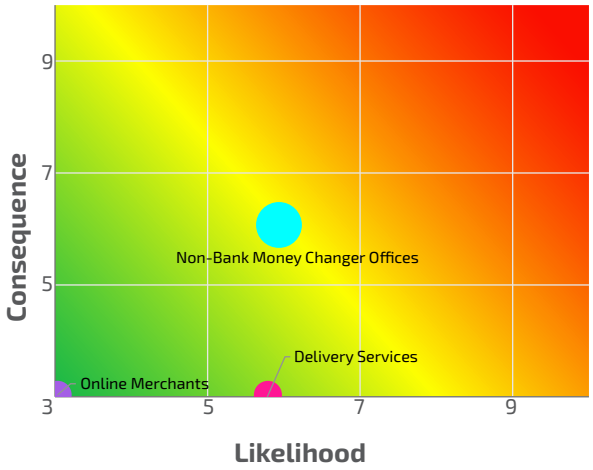
Terrorist financing risk was also assessed based on the delivery channel to ascertain which delivery channels were most at risk to cases of terrorist financing in non-bank money changers. The delivery channels as objects of this risk assessment are grouped into two main categories, namely the offices of non-bank money changers and delivery services. With the development of digital technology, however, unlicensed non-bank money changers have been found buying and selling foreign banknotes via online merchants, thus necessitating a risk assessment of this new delivery channel.

Using risk factors in the form of risk, the level of terrorist financing risk for each delivery channel in non-bank money changers was assessed and the results are presented in Table 2.10.

The results of mapping terrorist financing risk in the non-bank money changer sector by delivery channel is presented in Figure 2.9.

According to the TF risk heatmap presented in Figure 2.9, **Non-Bank Money Changer Offices** are a **high**-risk delivery channel for terrorist financing in the non-bank money changer sector, while other delivery channels are **low** risk.

Figure 2.9. TF Risk Heatmap by Delivery Channel in Non-Bank Money Changer Sector



Non-Bank Money Changer Offices recorded the highest risk scores compared with other delivery channels. Court reports from 2019-2020 also showed that non-bank money changer offices were the delivery channel invariably used for terrorist financing purposes.

Delivery Services and **Online Merchants** are low risk but the results of a risk assessment by reporting parties showed a medium risk posed by the delivery services channel. Meanwhile, **Online Merchants** received a high vulnerability score due to ineffective AML/CFT implementation in terms of mitigating terrorist financing risk using this delivery channel.

Table 2.10. Risk Analysis of Terrorist Financing in Non-Bank Money Changers by Delivery Channel

No	Product	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-Bank Money Changer Offices	6.00	8.73	6.00	6.00	**6,00**	Medium
2.	Delivery Services	8.00	9.00	3.00	5.89	**3,00**	Low
3.	Online Merchants	3.67	3.00	3.04	3.00	**3,02**	Low

3

RISK MITIGATION

A. Institutional Aspects of Risk Mitigation

1. Non-bank money changers in Indonesia must be licensed by Bank Indonesia.

2. Non-bank money changers are not permitted to perform other business activities, including money transfers.

3. Non-bank money changers, the management and shareholders of non-bank money changers are not permitted to have a business relationship or transact with unlicensed non-bank money changers.

4. Management and shareholders of non-bank money changers are required to meet the following requirements set by Bank Indonesia:

    a. Not included on the National Blacklist (DHN)[31] for withdrawals of blank cheques and/or money transfers.

    b. Not a debtor with non-performing loans (NPL) based on the Financial Information Services System (SLIK) of the Financial Services Authority (OJK).

    c. Fulfilled tax obligations as evidenced by a valid tax certificate issued by the tax authority within the last one year.

    d. Not convicted of a crime in the last two years.

    e. Not a shareholder, director or member of board of commissioners of a limited liability company subject to administrative sanctions in the form of licence revocation by Bank Indonesia within a period of two years prior to the date of application.

    f. Never been declared bankrupt.

    g. Not a shareholder, director or member of board of commissioners of a company declared bankrupt within a period of two years prior to the date of application.

5. Shareholders of non-bank money changers must be Indonesian citizens and/or business entities owned by Indonesian citizens.

6. Paid-up capital in non-bank money changers cannot be obtained from and/or used for money laundering.

7. A licence for a non-bank money changer is valid for five years from the date of the licence and may be extended via an application to Bank Indonesia.

8. Non-bank money changers are required to maintain a bank account in the name of the non-bank money changer.

9. In the licensing process for non-bank money changers, Bank Indonesia will check the licensing requirements of applicants, including confirming and requesting information from relevant authorities and institutions.

B. Operational Aspects of Risk Mitigation

a. Pre-Transaction Mitigation Measures

1. The activities of non-bank money changers are as follows:

31 In accordance with Bank Indonesia Regulation (PBI) No. 18/43/PBI/2016, as an amendment to Bank Indonesia Regulation (PBI) No. 8/29/PBI/2006 concerning the National Blacklist for Withdrawals of Blank Cheques and/or Money Transfers.

a. Exchanging foreign banknotes,

b. Purchasing traveller's cheques, and

c. Other business activities relating to non-bank money changers as stipulated in Bank Indonesia regulations.

2. Non-bank money changers are required to implement risk-based AML/CFT in the following operational activities:

   a. Tasks and responsibilities of Directors and active supervision of Board of Commissioners.

   b. Policies and written procedures.

   c. Risk management process.

   d. Management of human resources.

   e. Internal control system.

3. Directors and Board of Commissioners supervise AML/CFT program implementation.

4. Non-bank money changers implement customer due diligence in terms of customer identification and verification.

5. Non-bank money changers implement enhanced due diligence for high-risk prospective customers, customers and beneficial owners.

6. Non-bank money changers identify, assess, control and mitigate risk.

7. Non-bank money changers implement employee screening, customer due diligence and employee capacity building. Non-bank money changers appoint specialised employees for AML/CFT implementation.

8. Non-bank money changers implement robust internal control measures, including regular independent audits, to test AML/CFT implementation compliance and effectiveness.

9. Non-bank money changers administrate, update and confirm the accuracy of customer information, particularly high-risk customer profiles.

10. Non-bank money changers have access to various independent and reliable sources of data to verify customer profiles, including data from the Directorate General of Population and Civil Registration of Indonesia, as well as access to international databases, such as World-Check.

11. Non-bank money changers have access to the database of Politically Exposed Persons (PEP) administrated by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

b. Transaction Mitigation Measures

1. Foreign banknotes must be handed over in person.

2. Interbank and intrabank rupiah money transfers must be addressed to or from an account in the name of the non-bank money changer or customer.

3. Customer purchases of foreign banknotes exceeding USD25,000 or equivalent within one month must be accompanied by an underlying transaction.

4. Non-bank money changers are not permitted to recirculate SGD10,000 denomination banknotes.

5. Non-bank money changers may only accept interbank and intrabank rupiah money transfers addressed to or from an account in the name of the non-bank money changer or customer. If a different account is used, the non-bank money changer must request additional supporting documents to authorise the transaction.

c. Post-Transaction Mitigation Measures

1. Non-bank money changers manage data, information and documents as well as monitor transactions, which includes updating customer profiles and customer transaction profiles. Transaction monitoring includes due diligence of walk-in customers.

2. Non-bank money changers identify and red flag unusual transaction patterns.

3. Non-bank moneychangers identify and report suspicious transactions to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

d. Additional Risk Mitigation Measures Relating to Terrorist Financing

1. Non-bank money changers block or freeze funds belonging to individuals or corporations identified on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).

2. Non-bank money changers conduct rigorous investigations concerning the modus operandi and typologies of terrorist financing cases used by terrorist groups for more effective preventative measures.

3. Non-bank money changers administrate and update the List of Suspected Terrorists and Terrorist Organisations (DTTOT) and relevant UN Security Council Resolutions based on automatic screening to mitigate terrorist financing.

4. Non-bank money changers subscribe to international databases, such as World-Check, in relation to Politically Exposed Persons (PEP) and the List of Suspected Terrorists and Terrorist Organisations (DTTOT) in order to mitigate terrorist financing.

5. Non-bank money changers implement enhanced due diligence for high-risk prospective customers, customers and beneficial owners to mitigate the exploitation of immediate family members, including wives, children and others, to finance terrorism.

6. In terms of collaborating with third parties, such as agents or partners, non-bank money changers ensure adequate AML/CFT implementation by the third party, including money transfers to and from Indonesia indicated for terrorism, terrorists and terrorist organisations.

C. Supervision Aspects of Risk Mitigation

1. Bank Indonesia conducts direct and indirect risk-based supervision in relation to AML/CFT implementation by non-bank money changers. Intensive supervision is applied to the customer due diligence and record keeping processes implemented by non-bank money changers.

2. Bank Indonesia performs thematic supervision of non-bank money changers.

3. Bank Indonesia may assign other parties for and on behalf of Bank Indonesia to perform supervisions of non-bank money changers.

4. Concerning supervision by Bank Indonesia, non-bank money changers must identify, manage and update data concerning Beneficial Owners, while ensuring the availability of data on Beneficial Owners in the interest of Bank Indonesia supervision.

4

CONCLUSIONS

A. Money Laundering Risks

Based on the outcome of statistical data analysis and the risk score of sectoral money laundering in non-bank money changers by **region (province), customer profile, product** and **service** as well as **delivery channel**, the following conclusions were drawn:

1. The **Special Capital Region of Jakarta** and province of **Riau Islands** are **high-risk** regions in terms of money laundering using non-bank money changers, followed by the provinces of **West Java, Banten, East Java** and **North Sumatra** as **medium-risk** regions. All other provinces are **low** risk.

2. **Politically Exposed Persons (PEP), Private Sector Employees** and **Entrepreneurs** are **high-risk** individual customers for money laundering activity in non-bank money changers, followed **Money Changer Employees** as **medium** risk. All other individual customer profiles are **low** risk.

3. **Non-MSME Limited Liability Companies (PT)** and **Limited Partnership Companies (CV)** are **high-risk** institutional customers for money laundering activity in non-bank money changers, followed by **Government Institutions** as **medium** risk. All other institutional customers are **low** risk.

4. **USD and SGD** are **high-risk** products (foreign banknotes) for money laundering activity in non-bank money changers, followed by **EUR, AUD** and **MYR** as **medium** risk. All other foreign banknotes are low risk.

5. **Non-Bank Money Changer Offices** are a **medium-risk** delivery channel for money laundering activity in non-bank money changers, with all other delivery channels considered **low** risk.

Table 2.11. Outcome of Sectoral Risk Assessment of Money Laundering in Non-Bank Money Changers

Risk	Province	Profession	Business Entity	Product	Delivery Channel
High	Special Capital Region of Jakarta, Riau Island	PEPs, Private Sector Employees, Entrepreneurs	Non-MSME Limited Liability Companies (PT), Non-MSME Limited Partnership Companies (CV)	USD, SGD	-
Medium	West Java, Banten, East Java, North Sumatra	Money Changer Employee	Government Institutions	EUR, AUD, MYR	Non-Bank Money Changer Offices
Low	Others	Others	Others	Others	Delivery Services, Online Merchants

B. Terrorist Financing Risk

Based on the outcome of terrorist financing risk analysis in non-bank money changers by **region (province), customer profile, product** and **service** as well as **delivery channel**, the following conclusions were drawn:

1. The **Special Capital Region of Jakarta** is a **high-risk** region for terrorist financing activity in non-bank money changers, followed by the provinces of **East Java** and **Papua** as **medium-risk** regions. All other provinces are **low** risk.

2. **Private Sector Employees** and **Entrepreneurs** are **high-risk** individual customers for terrorist financing activity in non-bank money changers, followed **Housewives** as **medium** risk. All other individual customers are **low** risk.

3. **USD** is a **high-risk** product (foreign banknote) for terrorist financing activity in non-bank money changers, followed by **SGD** as **medium** risk. All other foreign currencies are **low** risk.

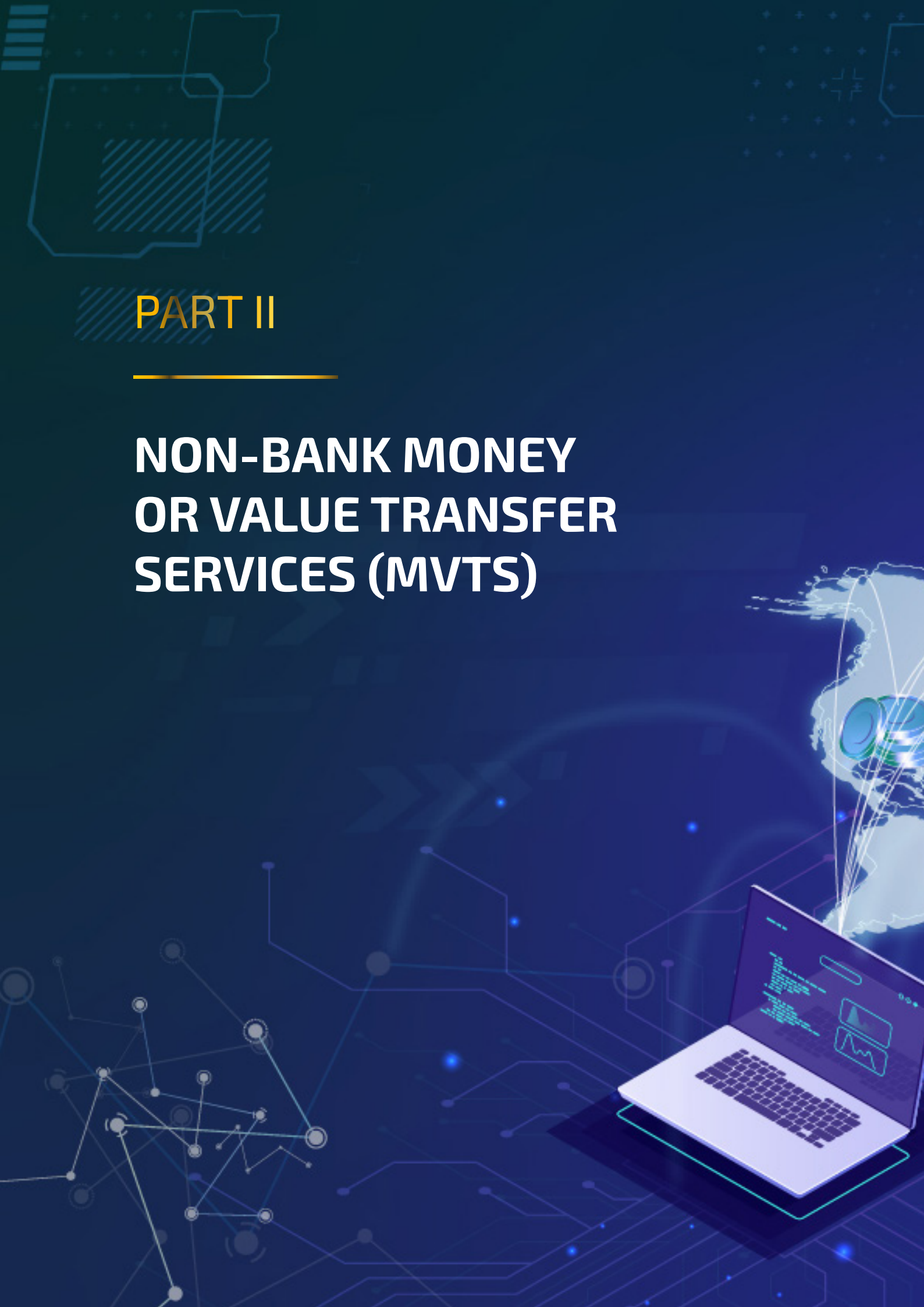
4. **Non-Bank Money Changer Offices** are a **medium-risk** delivery channel for terrorist financing activity in non-bank money changers, with all other delivery channels considered **low** risk.

Table 2.12. Outcome of Sectoral Risk Assessment of Terrorist Financing in Non-Bank Money Changers

Risk	Province	Profession	Product	Delivery Channel
High	Special Capital Region of Jakarta	Private Sector Employees , Entrepreneurs	USD	-
Medium	East Java, Papua	Housewife	SGD	Non-Bank Money Changer Offices
Low	Others	Others	Others	Delivery *Services*, Online Merchants

PART II

NON-BANK MONEY OR VALUE TRANSFER SERVICES (MVTS)



Executive Summary

In 2021, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), in conjunction with relevant government ministries/ agencies, identified, analysed and evaluated the latest money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks holistically through the national risk assessment program, namely the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021. Based on the NRA of Money Laundering 2021, Non-Bank Money or Value Transfer Services (MVTS) are considered a medium-risk industry.

As a follow-up action to mitigate the risk of money laundering, terrorist financing and proliferation financing of WMD in non-bank Money or Value Transfer Services, a sectoral risk assessment (SRA) of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction was performed covering non-bank Money or Value Transfer Services with the following objectives:

1. Identifying and analysing the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank Money or Value Transfer Services.

2. Identifying, analysing and evaluating various risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction based on risk mapping the customers (individual and corporate), regions (provinces), products and services as well as delivery channels of non-bank Money or Value Transfer Services.

3. Identifying and analysing the emerging threats of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank Money or Value Transfer Services.

4. Formulating strategic risk mitigation measures against money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank Money or Value Transfer Services.

The SRA of non-bank Money or Value Transfer Services mapped four key risks based on customer profile, region, product and service as well as delivery channel and formulated risk factors covering the threats, vulnerabilities and consequences. The analysis methodology referred to the risk assessment method published by the Financial Action Task Force (FATF).

According to the latest assessment, the level of money laundering risk in non-bank Money or Value Transfer Services is as follows:

1. The **Special Capital Region of Jakarta** is a **high-risk** region for money laundering activity in non-bank Money or Value Transfer Services, followed by the provinces of **West Java, Riau Islands, East Java** and **Central Java** as **medium-risk** regions. All other provinces are **low** risk.

2. **Non-MSME Limited Liability Companies (PT)** are **high-risk** institutional customer profiles for money laundering activity in non-bank Money or Value Transfer Services, followed by **Government Institutions** as **medium** risk. All other institutional customer profiles are **low** risk.

3. **Entrepreneurs, Private Sector Employees** and **Politically Exposed Persons (PEP)** are **high-risk** individual customer profiles for money laundering activity in non-bank Money or Value Transfer Services, followed **Housewives, Professionals** and **Consultants** as **medium** risk. All other individual customer profiles are **low** risk.

4. **Cash to Account (outgoing)** is a **high-risk** product for money laundering activity in non-bank Money or Value Transfer Services, followed by **Account to Account (incoming)** as **medium** risk. All other products and services of non-bank Money or Value Transfer Services are **low** risk.

5. **Non-Bank Money or Value Transfer Services** are a **medium-risk** delivery channel for money laundering activity in non-bank Money or Value Transfer Services, followed by **Agents** and **Mobile Applications** as **low**-risk delivery channels.

Based on the latest assessment, the level of terrorist financing risk in non-bank Money or Value Transfer Services is as follows:

1. The **Special Capital Region of Jakarta** and **Riau Islands** are **high-risk** regions for terrorist financing activity in non-bank Money or Value Transfer Services, followed by the provinces of **West Java** and **East Java** as **medium-risk** regions. All other provinces are **low** risk.

2. **Entrepreneurs** are a **high-risk** individual customer profile for terrorist financing activity in non-bank Money or Value Transfer Services, followed **Private Sector Employees** as **medium** risk. All other individual customer profiles are **low** risk.

3. **Cash to Cash (outgoing, incoming, domestic)** is a **high-risk** product for terrorist financing activity in non-bank Money or Value Transfer Services, followed by **Account to Account (outgoing)** as **medium** risk. All other products and services are **low** risk.

4. **Non-bank Money or Value Transfer Services** are a **medium-risk** delivery channel for terrorist financing activity in non-bank Money or Value Transfer Services, followed by **Agents** and **Mobile Applications** as **low-risk** delivery channels.

Seeking to mitigate the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank Money or Value Transfer Services, Bank Indonesia has issued regulations and guidelines, while implementing direct oversight and indirect supervision. In conjunction with the Indonesian National Police, Bank Indonesia has shut down illegal and unlicensed non-bank Money or Value Transfer Services throughout Indonesia. In addition, Bank Indonesia has also provided socialisation and education activities targeting non-bank Money or Value Transfer Services and members of the public to increase awareness of the risks and support efforts to prevent and eradicate money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

1

LITERATURE REVIEW OF NON-BANK MONEY OR VALUE TRANSFER SERVICES

A. Legal Basis

Legally, Bank Indonesia is a supervisory and regulatory body (LPP) for non-bank Money or Value Transfer Services in accordance with Act No. 9 of 2013 concerning the Prevention and Eradication of Terrorist Financing (TF Act). Money transfer activity is regulated by Act No. 3 of 2011 concerning Money Transfers (Money Transfer Act). Discharging its mandate in accordance with the Money Transfer Act, Bank Indonesia issued Bank Indonesia Regulation (PBI) No. 14/23/PBI/2012 concerning Money Transfers and Bank Indonesia Circular Letter (SEBI) No. 15/23/DASP concerning Money or Value Transfer Services. The salient provisions of the Bank Indonesia Regulations on Non-Bank Money or Value Transfer Services are as follows:

1. Licensing of non-bank Money or Value Transfer Services.
2. Implementation of money transfers.
3. Payment of money transfers in cash.
4. Services, interest rates or compensation.
5. Money transfer fees.
6. Due diligence.
7. Sanctions

Since July 2021, however, regulations regarding payment system have been implemented in accordance with Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System as well as PBI No. 23/6/PBI/2021 concerning Payment Service Providers (PJP) and PBI No. 23/7/PBI/2021 concerning Payment System Infrastructure Provider (PIP). Based on the latest payment system regulations, Non-Bank Money or Value Transfer Services (MVTS) are permitted to provide remittance services in the form of accepting and executing money transfer orders for funds not originating from accounts administrated by remittance providers. Furthermore, provisions regarding the licensing of Money or Value Transfer Services are regulated in Bank Indonesia Regulation on Payment Service Provider which regulates the licence category, validity period, requirements, mechanisms and procedures as well as the granting of PJP licences.

B. Characteristics of Non-Bank Money or Value Transfer Services in Indonesia

1. Definition

Pursuant to Article 1, Paragraph (2) of Act Number 3 of 2011 concerning Money Transfers, non-bank Money or Value Transfer Services are banks and non-bank business entities incorporated in Indonesia to transfer funds. A license to transfer funds by banks is not required because money transfer services are already included as a banking activity in accordance with prevailing banking regulations.

Non-bank business entities are required, however, to obtain a license to operate as a non-bank money or value transfer services from Bank Indonesia through a written application submitted to Bank Indonesia in accordance with the procedures stipulated in the applicable Bank Indonesia regulation. Based on Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System, there has been an activity-based reclassification on the entry side. The licensing process has been streamlined to increase efficiency by bundling licence categories based on activity. The licensing requirements are as follows: (i) institution, (ii) capital and finance,

(iii) risk management, and (iv) information system capabilities.

A money order begins with the originator's payment order, which is forwarded to the correspondent and receiver and onto the beneficiary. In accordance with the Funds Transfer Act, Bank Indonesia performs due diligence on the operators in the form of direct surveillance and indirect monitoring. Direct surveillance includes regular inspections and/or as required, while indirect monitoring is performed based on the reports submitted by Money or Value Transfer Services.

2. Products and Services

The business activities of non-bank Money or Value Transfer Services are as follows:

c. Outgoing transfers (from Indonesia)

d. Incoming transfers (to Indonesia)

e. Domestic transfers (within Indonesia)

According to Bank Indonesia, from 2019-2020, transaction volume was dominated by domestic transfers, accounting for 90.56% of the total, with incoming and outgoing transfers accounting for just 9.27% and 0.17% respectively. Based on transaction value, however, domestic transfers accounted for just 51.21% of the total, with incoming and outgoing transfers accounting for 29.89% and 18.90% respectively.

Regarding the money transfer mechanism, a sender may choose to transfer funds via non-bank Money or Value Transfer Services in cash or by debiting the sender's account. The non-bank money or value transfer services can then deliver the funds to the beneficiary in cash or by crediting the beneficiary account in accordance with the sender's instructions.

3. Delivery Channels

To initiate a money transfer transaction via a non-bank money or value transfer services, the customer must send and/or receive funds directly from a non-bank money or value transfer services office and/or through an agent of the non-bank money or value transfer services. In line with the advancement of technology, a customer can now send and/or receive funds via a mobile application developed by a non-bank money or value transfer services.

4. Regional Distribution

Based on distributional data, non-bank Money or Value Transfer Services remain concentrated in the Special Capital Region of Jakarta, followed by the Riau Islands, West Java, North Sumatra and East Java. In terms of transaction value, as of December 2021, transactions via non-bank Money or Value Transfer Services were also concentrated in those five provinces, with Jakarta accounting for 42%.

The distribution of non-bank Money or Value Transfer Services Indonesia is recapitulated as follows:

Table 3.1. Distribution of Non-Bank Money or Value Transfer Services as of December 2021

No	Province	Total
1	Special Capital Region of Jakarta	67
2	Riau Islands	61
3	West Java	14
4	North Sumatra	9
5	East Java	8
6	West Kalimantan	6
7	Banten	3
8	East Java	3
9	Bali	2
10	East Nusa Tenggara	1
11	West Nusa Tenggara	1
12	West Sumatra	1
13	Lampung	1
14	Yogyakarta Special Region	1
Total		**178**

Source: Bank Indonesia

2

KEY RISKS IN NON-BANK MONEY OR VALUE TRANSFER SERVICES

A. Money Laundering Risk Landscape

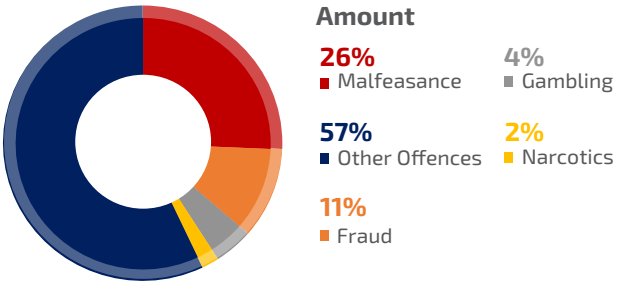
Based on the National Risk Assessment (NRA) of Money Laundering 2021, non-bank Money or Value Transfer Services are a medium-risk industry. The predicate crimes seek to exploit weaknesses in non-bank Money or Value Transfer Services in order to conceal the illicit proceeds of crime. Based on Suspicious Transaction Reports (STR) for the period from 2019-2020, most predicate offenses indicating use of non-bank Money or Value Transfer Services are linked to malfeasance and fraud. Furthermore, money laundering typologies in Indonesia have also involved cross-border transactions, primarily using non-bank Money or Value Transfer Services with extensive international networks, including in high-risk countries.

Based on data and information obtained from the analysis of court reports by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), several money laundering typologies using non-bank Money or Value Transfer Services were identified as follows:

1. Licensed non-bank Money or Value Transfer Services cooperating with unlicensed non-bank Money or Value Transfer Services to send or receive funds.

2. High-frequency transactions of relatively small value during a given period (structuring).

Graph 3.1. Composition of Predicate Offences based on Suspicious Transaction Reports in Non-Bank Money or Value Transfer Services



3. Outgoing transfers from several non-bank Money or Value Transfer Services to the same beneficiary.

4. Non-bank money or value transfer services transactions that are inconsistent with current business activity. For example, a non-bank money or value transfer services established to transfer funds from Indonesian migrant workers (PMI) yet appearing not to receive any significant foreign exchange transactions from abroad, with the business account dominated by domestic transactions.

5. Receiving incoming transactions, followed immediately by outgoing transactions.

6. Using false identity documents or creating fictitious or invalid data.

7. Redeeming funds using several accounts (smurfing)

Examples of money laundering cases involving non-bank Money or Value Transfer Services are as follows:

Criminal case against EA (North Jakarta District Court Case Number: 1106/Pid.Sus/2019/PN.Jkt.Utr) for money laundering with the predicate offence of fraud and the following typology:

a. Defendant EA cooperated to commit fraud with a foreign national, DM, domiciled in Indonesia. DM was known to use social media to defraud victims located abroad. DM sought out victims who could open bank accounts in Indonesia to accommodate incoming transfers of funds from abroad as the illicit proceeds of fraud crime.
b. EA redeemed the illicit proceeds of crime sent to Indonesia via non-bank Money or Value Transfer Services using several of his own bank accounts and bank accounts owned by others using false identification documents.

Criminal case against PB and CPM (Central Jakarta District Court Case Number: 1106/Pid.Sus/2019/PN Jkt.Pst) for money laundering with the predicate offences of theft and fraud and the following typology:

a. Defendants PB and CPM cooperated with a German national (AM) to create fictitious transactions. AM initiated online retail transactions via a website owned by PB, paid for using other people's credit cards by illegally accessing the electronic documents of the credit card owners.

b. The payments to PB's bank account from the fictitious transactions were withdrawn in cash by defendant CPM and sent to AM via an outgoing transfer through a non-bank money or value transfer services.

B. Terrorist Financing Risk Landscape

In the context of terrorist financing, terrorist groups can exploit industry weaknesses through specific typologies to fund terrorist acts. Terrorist groups exploit non-bank Money or Value Transfer Services to transfer funds, namely using incoming and/or outgoing transfers, to fund terrorist acts. Domestic and cross-border transfers through non-bank Money or Value Transfer Services are used. Based on the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021, non-bank Money or Value Transfer Services received high risk scores in terms of the threat and consequence concerning money transfers because non-bank Money or Value Transfer Services have expansive domestic and international networks, including in high-risk countries and/or regions.

The advancement of technology has created a paradigm shift in terms of terrorist financing from conventional to digital methods. The National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021 found that terrorist groups have started exploiting virtual payment instruments to finance terrorism because virtual payments can be sent and/or received by anyone with an internet connection. The virtual funding method utilises funds via online lending or payments via e-commerce platforms. Furthermore, terrorist groups are already using legitimate business entities. Terrorist acts are also supported by cross-border funding.

There are several terrorist financing and proliferation financing of WMD typologies using non-bank Money or Value Transfer Services based on data and information obtained from the analysis of court reports by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) as follows:

1. Digital fundraising through transfers or cash by misusing non-bank Money or Value Transfer Services with global foreign branches or agents.

2. The use of relatives' or colleagues' names to obscure the detection process.

Several examples of terrorist financing cases involving non-bank Money or Value Transfer Services have been identified as follows:

1. Terrorists on behalf of BN received terrorist financing funds through non-bank Money or Value Transfer Services sent from Australia, Malaysia, Singapore and the Philippines.
2. Leaders of terrorist groups from Indonesia on behalf of BRS in Syria channelled funds to terrorist groups in Marawi, the Philippines, via non-bank Money or Value Transfer Services from the Middle East to Indonesia and then on to the Philippines.

C. Money Laundering Risk Assessment Analysis

1. Money Laundering Risk by Region

A risk assessment of money laundering in non-bank Money or Value Transfer Services was performed based on region to ascertain which provinces were the highest risk of money laundering cases paying due regards to the outcome of the National risk assessment. The sectoral risk assessment by region measured the threats, vulnerabilities and consequences in each respective province based on predetermined risk factors.

Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability. The main results of the sectoral risk assessment by region of money laundering in non-bank Money or Value Transfer Services are recapitulated in Table 3.2.

The results of mapping money laundering risk in non-bank Money or Value Transfer Services by region is presented in Figure 3.1.

Figure 3.1. ML Risk Heatmap by Region in MVTS Sector

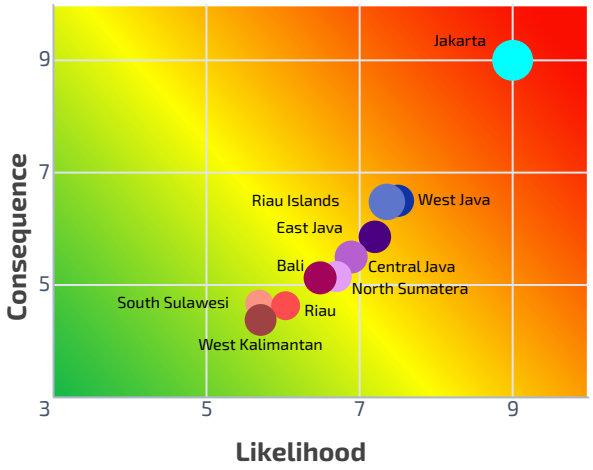


Table 3.2. Analysis of Money Laundering in MVTS Sector by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Jakarta	9.00	9.00	9.00	9.00	**9.00**	High
2.	West Java	6.98	7.98	6.50	7.48	**6.97**	Medium
3.	Riau Island	7.85	6.82	6.48	7.34	**6.89**	Medium
4.	East Java	6.90	7.50	5.85	7.20	**6.49**	Medium
5.	Central Java	6.32	7.46	5.50	6.89	**6.15**	Medium
6.	Others	4.38	5.83	4.16	5.11	**4.60**	Low

Based on the risk heatmap presented in Figure 3.1, **Jakarta** is the only province with a **high** level of money laundering risk in non-bank Money or Value Transfer Services, followed by **West Java, Riau Islands, East Java** and **Central Java** as **medium**-risk regions. All other 29 regions are **low** risk.

Jakarta recorded the highest scores for risk compared to other regions, while **West Java, East Java** and **Central Java** received medium scores for threat and consequence yet high in terms of vulnerability. The **Riau Islands** is considered a medium-risk region due to a high threat score.

The high threat and consequence scores in Jakarta and high threat score in Riau Islands stemmed from the comparatively large number of money laundering cases discovered in those provinces based on Suspicious Transaction Reports (STR) and Cash Transaction Reports (CTR) as well as court reports from 2019-2020. In addition, both provinces have a relatively high concentration of non-bank Money or Value Transfer Services. According to Bank Indonesia data from 2019-2020, West Java dominated the value and volume of incoming money transfer transactions from abroad, accounting for 27% and 8% of the total respectively.

The high vulnerability score was influenced by the level of AML/CFT implementation in the region, coupled with the perception of law enforcement agencies concerning constraints to case handling in areas where the transactions occur. The potential risks in the five aforementioned regions are also higher than in other regions due to their status as business, economic, financial and government centres. Furthermore, proximity to international borders also exposes those regions to money laundering risk.

Money laundering crime in Indonesia using non-bank Money or Value Transfer Services also involves cross-border transactions. Based on the National Risk Assessment of Money Laundering 2021, the highest risk countries of laundering offshore or outward risk were Singapore, United States, India, China, Thailand, Malaysia and Hong Kong, while the countries with high inward risk are Malaysia, Japan, Singapore, Thailand, Saudi Arabia and the United Arab Emirates.

According to the FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services published in 2016, no universal definition or methodology has been put forward to determine which countries or geographical locations are high risk in terms of money laundering. Notwithstanding, a range of factors may indicate risk as follows:

a. Countries or areas identified as having significant levels of corruption, narcotics (including source or transit countries for illegal drugs), human trafficking and illegal gambling based on the latest credible and independent documents and/or information sources.

b. Countries subject to sanctions, embargoes or similar measures issued by international organisations, such as the United Nations.

c. Countries identified as having weak governance, law enforcement and regulatory regimes, including countries identified by FATF Statements as having weak AML/CFT regimes based on the latest credible and independent documents and/or information sources.

2. Money Laundering Risk by Corporate Customer Profile

According to money laundering risk analysis based on customer in the National Risk Assessment of Money Laundering 2021, corporate and individual customer profiles were shown to be high risk domestically. Therefore, a risk analysis of money laundering based on business entity was necessary to understand which types of corporate customer profile were most at risk of money laundering in non-bank Money or Value Transfer Services.

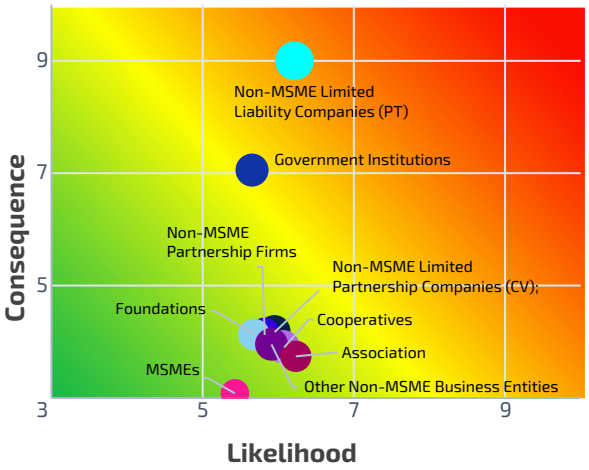
The results of money laundering risk analysis in non-bank Money or Value Transfer Services based on corporate customer profile are presented in Table 3.3.

The results of mapping money laundering risk in non-bank Money or Value Transfer Services by corporate customer profile are presented in Figure 3.2

According to the risk heatmap presented in Figure 3.2, **Non-MSME Limited Liability Companies (PT)** are **high** risk for money laundering in non-bank Money or Value Transfer Services, while **Government Institutions (including state/regional enterprises)** are **medium** risk. All other business entities are **low** risk.

Non-MSME Limited Liability Companies (PT) and **Government Institutions** recorded the highest risk score compared to other corporate customer profiles. This was reflected in court

Figure 3.2. Risk Heatmap by Corporate Customer Profile in MVTS Sector



report data from 2019-2020, showing that both types of customer profile dominated money laundering cases using non-bank Money or Value Transfer Services. Meanwhile, the high consequence scores were due to the significant impact posed by money laundering on the financial system and economy.

3. Money Laundering Risk based on Individual Customer Profile

Money laundering risk was also assessed based on individual customer profile to ascertain which professions were most at risk to committing money laundering via non-bank Money or Value Transfer Services. The customer profiles used in this assessment refer to the National Risk Assessment of Money Laundering

Table 3.3. Risk Analysis of Money Laundering in MVTS Sector by Corporate Customer Profile

No	Customer Profile	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-MSME Limited Liability Companies (PT)	7.31	5.12	9.00	6.22	7.48	High
2.	Government Institutions	5.02	6.29	7.06	5.65	6.32	Medium
3.	Others	6.02	5.72	3.87	5.87	4.76	Low

in 2021. The risk assessment based on individual customer profile for non-bank Money or Value Transfer Services had the following limitations:

a. The obligations of non-bank Money or Value Transfer Services to administrate customer information in accordance with Article 51, Paragraph (1) of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Implementation of Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) for Payment Service Providers and Non-Bank Money Changers.

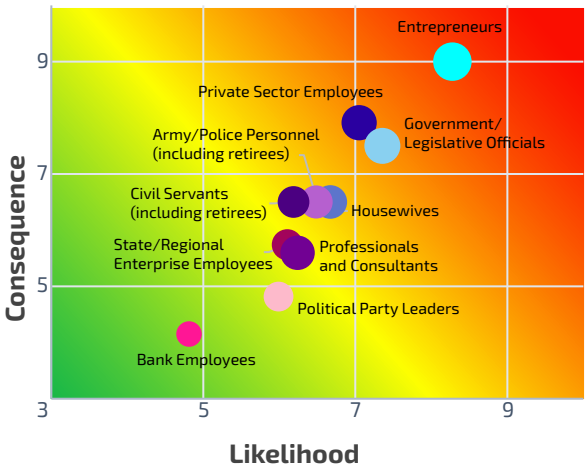
b. The dominance of walk-in customers at non-bank Money or Value Transfer Services.

According to the risk scores, the results of money laundering risk analysis in non-bank Money or Value Transfer Services based on individual customer profile are presented in Table 3.4.

The results of mapping money laundering risk in non-bank Money or Value Transfer Services by individual customer profile are presented in Figure 3.3

According to the risk heatmap presented in Figure 3.4, **Entrepreneurs, Private Sector Employees** and **Government/Legislative Officials** are high risk in terms of money

Figure 3.3. ML Risk Heatmap by Individual Customer Profile in MVTS Sector



laundering in non-bank Money or Value Transfer Services, while **Housewives**, **Army/ Police Personnel (including retirees), Civil Servants (including retirees), State/Regional-**

Table 3.4. Risk Analysis of Money Laundering in MVTS Sector by Individual Customer Profile

No	Perorangan	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Entrepreneurs	9.00	7.55	9.00	8.28	**8.63**	High
2.	Private Sector Employees	8.16	5.94	7.93	7.05	**8.15**	High
3.	Government/Legislative Officials	6.21	8.50	7.50	7.36	**8.07**	High
4.	Housewives	6.52	6.85	6.50	6.68	**6.59**	Medium
5.	Army/Police Personnel (including retirees)	6.42	6.33	6.50	6.38	**6.44**	Medium
6.	Civil Servants (including retirees)	6.65	5.97	6.50	6.31	**6.40**	Medium
7.	State/Regional Enterprise Employees	6.19	6.02	5.74	6.11	**5.92**	Medium
8.	Professionals and Consultants	5.74	6.74	5.59	6.24	**5.90**	Medium
9.	Political Party Leaders	5.08	6.90	4.82	5.99	**5.37**	Medium
10.	Other Professions	4.64	5.02	4.24	4.83	**4.53**	Low

Owned Enterprise Employees (including retirees), Professionals and Consultants as well as **Political Party Leaders** are considered **medium**-risk customer profiles.

Entrepreneurs and Private Sector Employees recorded the highest threat and consequence scores based on suspicious transaction reports, cash transaction reports and court reports from 2019-2020, considering most customers of non-bank Money or Value Transfer Services are Entrepreneurs and Private Sector Employees. According to the risk analysis, Entrepreneurs and Private Sector Employees are high risk due to the involvement of both customer profiles in business activity, including illegal activity.

Pursuant to Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Combating The Financing of Terrorism for Non-Bank Payment Service Providers and Non-Bank Money Changers, and referring to FATF Guidance on Politically Exposed Persons (PEP), customer profiles included in the category of Politically Exposed Persons are particularly vulnerable to money laundering. Therefore, prospective customers, customers and beneficial owners categorised as PEP are treated as high-risk customers. As reported in the National Risk Assessment of Money Laundering 2021, customer profiles categorised as Domestic PEP include **Government/Legislative Officials, State/Regional-Owned Enterprise Employees (including retirees), Civil Servants (including retirees)** and **Army/Police Personnel (including retirees).** Political Party Leaders are also highly vulnerable due to their authority and function as government/legislative officials. In addition to domestic PEP, foreign PEPs are also high risk in terms of laundering offshore foreign outward risk using non-bank Money or Value Transfer Services.

Housewives as well as Professionals and Consultants are medium risk for money laundering in non-bank Money or Value Transfer Services. In terms of threat and consequence, court reports show that housewives used non-bank Money or Value Transfer Services as a means of money laundering in the period from 2019-2020. Based on Strategic Analysis of Professionals and Consultants as well as Housewives performed by the Financial Monitoring Unit of the Government of Pakistan, both profiles pose a money laundering risk using the names of clients and/or family members to conceal the identity of the beneficial owner using the illicit proceeds of crime.

According to the FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services published in 2016, the following activities may indicate a high risk of money laundering:

a. Customer is another Non-Bank money or value transfer services or Payment Service Provider that has been sanctioned by the respective national competent authority for its non-compliance with the AMF/CFT applicable regime.

b. Customer conducting a business relationship or transactions in unusual circumstances, such as:

   i. Customer who travels unexplained distances to locations to conduct transactions.

   ii. Defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services.

   iii. Customer owns or operates a cash-based business that appears to be a front or shell company or is intermingling legal and illicit proceeds as determined from a review of transactions that seem inconsistent with the financial standing or business profile.

c. Politically exposed person or his/her family members or close associates.

d. Non-face-to-face customer, where doubts exist about the identity of such a customer.

e. Customer who uses agents or associates where the nature of the relationship or transaction makes it difficult to identify the beneficial owner of the funds.

f. Customer knows little or is reluctant to disclose details about the payee (contact information, address and other information).

g. Consumer gives inconsistent information, such as providing different names.

h. Customer involved in a transactions that has no apparent ties to the destination country and with no reasonable explanation.

i. Suspicion that the customer is acting on behalf of a third party but not disclosing that information or is being controlled by someone else. For example, the customer collects a money transfer and immediately hands it to someone else.

j. Customer has been the subject of law enforcement sanctions.

k. Customer offers false/fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents.

l. Customer whose transactions and activities indicate connection with potential criminal involvement, typologies or red flags provided in reports produced by the FATF or Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

m. Customer whose transaction patterns appear consistent with the generation of criminal proceeds, for example, illegal drug growing season, period of immigrant worker departures, corruption, based on information available with the MVTS.

4. Money Laundering Risk based on Products and Services

Money laundering risk was also assessed based on the products and services to ascertain which were most at risk to cases of money laundering in non-bank Money or Value Transfer Services. The products of non-bank Money or Value Transfer Services are outgoing transfers (from Indonesia), incoming transfers (to Indonesia) and domestic transfers (within Indonesia). In addition, money transfer mechanisms include cash to cash, cash to account, account to cash and account to account. In total, therefore, 12 products and services of non-bank Money or Value Transfer Services were assessed in terms of money laundering risk.

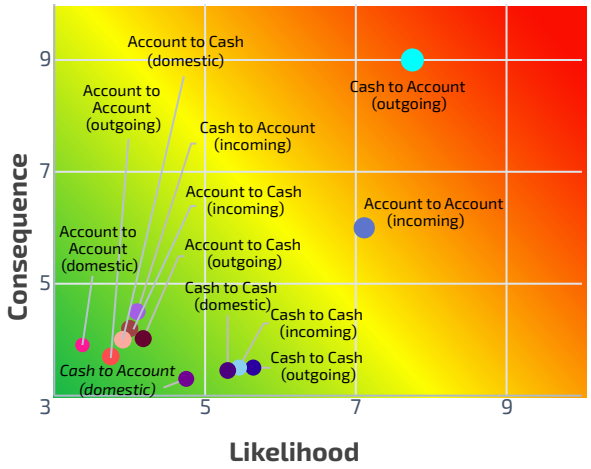
The results of money laundering risk analysis in non-bank Money or Value Transfer Services based on the products and services using several risk factors in the form of risk are presented in Table 3.5.

Table 3.5. Risk Analysis of Money Laundering in MVTS Sector by Product and Service

No	Product or Service	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Cash to Account (Outgoing)	9.00	6.00	9.00	7.50	8.22	High
2.	Account to Account (Incoming)	8.23	6.00	6.00	7.11	6.53	Medium
3.	Others	3.84	5.55	3.77	4.70	4.21	Low

The results of mapping money laundering risk in non-bank Money or Value Transfer Services by product and service is presented in Figure 3.4.

Figure 3.4. ML Risk Heatmap by Product and Service in MVTS Sector



According to the risk heatmap presented in Figure 3.4, **Cash to Account (outgoing)** is a **high**-risk product for money laundering in non-bank Money or Value Transfer Services, while **Account to Account (incoming)** is **medium** risk. All other products and services are **low** risk.

Cash to Account (outgoing) and **Account to Account (incoming)** products recorded the highest values of threat and consequence compared to the other products. Court reports from 2019-2020 indicate cases of money laundering using both products and services. The high frequency and value of suspicious transactions increased the level of threat and consequence of both products.

Cash is considered more vulnerable than cashless due to traceability issues. Notwithstanding, based on an SRA survey of sample non-bank Money or Value Transfer Services, most licensed non-bank Money or Value Transfer Services are implementing effective AML/CFT policy for all products and services.

According to the FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services published in 2016, the following products and services may indicate a high risk of money laundering:

1. Products or services that may inherently favour anonymity or products that can readily cross international borders, such as cash and online money orders, to beneficiaries with unverified identities.

2. Products or services that have a very high transaction limit.

3. Products and services with global reach.

4. Complex products and services.

5. Products and services that permit the exchange of cash for a negotiable instrument, such as a money order or chip-based electronic money.

5. Money Laundering Risk based on Delivery Channel

Money laundering risk was also assessed based on the delivery channel to ascertain which were most at risk to cases of money laundering in non-bank Money or Value Transfer Services. The delivery channels of non-bank Money or Value Transfer Services are the channels by which customers hand over and/or collect funds to be sent and/or received.

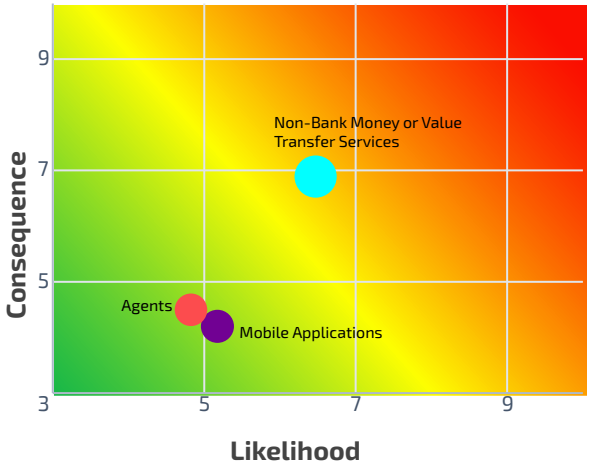
Using risk factors in the form of risk, the level of risk for each delivery channel in the MVTS sector was assessed and the results are presented in Table 3.6.

Table 3.6. Risk Analysis of Money Laundering in MVTS Sector by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-Bank Money or Value Transfer Services	6.80	6.14	6.90	6.47	**6.68**	Medium
2.	Other Delivery Channels	3.90	6.45	4.35	5.17	**4.74**	Low

The results of mapping money laundering risk in non-bank Money or Value Transfer Services by delivery channel is presented in Figure 3.5.

Figure 3.5. ML Risk Heatmap by Delivery Channel in MVTS Sector



According to the risk heatmap presented in Figure 3.5, **Non-Bank Money or Value Transfer Services** are a **medium-risk** delivery channel for money laundering in non-bank Money or Value Transfer Services, while **Agents** and **Mobile Applications** are **low-risk** delivery channels.

Non-Bank Money or Value Transfer Services recorded the highest risk scores compared to other delivery channels. Court reports from 2019-2020 showed that non-bank money or value transfer services offices were the delivery channel used for money laundering purposes.

The results of a risk assessment by law enforcement agencies showed a higher level of vulnerability concerning Mobile Applications than other delivery channels due to the ease and convenience of using mobile applications as well as ease of using false identification through mobile applications to conceal the identity of the beneficial owner.

D. Terrorist Financing Risk Assessment Analysis

1. Risk Analysis by Region

Terrorist financing risk in the MVTS sector was assessed by region to find out which provinces were most at risk of terrorist financing.
The risk analysis by region was performed based on the level of risk in each respective province, measured in accordance with the predetermined risk factors.

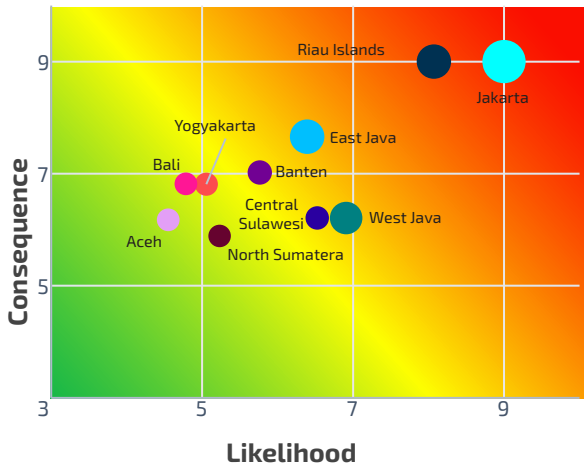
Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability scores. The salient results of the risk analysis by region of terrorist financing in non-bank Money or Value Transfer Services are presented in Table 3.7.

The results of mapping terrorist financing risk in non-bank Money or Value Transfer Services by region is presented in Figure 3.6

Table 3.7. Risk Analysis of Terrorist Financing in MVTS Sector by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Special Capital Region of Jakarta	9.00	9.00	8.95	9.00	9.00	High
2.	Riau Island	8.58	7.52	9.00	8.05	7.14	High
3.	West Java	6.95	6.88	6.21	6.90	6.83	Medium
4.	East Java	8.70	8.08	7.66	6.38	6.64	Medium
5.	Nanggroe Aceh Darussalam	4.26	4.94	6.15	4.56	5.00	Low
6.	Bali	5.32	4.29	6.79	4.77	4.96	Low
7.	Banten	5.94	5.86	7.02	5.87	4.83	Low
8.	Central Sulawesi	5.53	7.62	7.21	6.56	4.82	Low
9.	Special Region of Yogyakarta	5.96	4.20	6.77	5.05	4.81	Low
10.	Others	5,48	4,94	5,89	5,18	4,77	Low

Figure 3.6. TF Risk Heatmap by Region in MVTS Sector



Based on the risk heatmap presented in Figure 3.6, the **Special Capital Region of Jakarta** and **Riau Islands** are the provinces with a **high** level of terrorist financing risk in non-bank Money or Value Transfer Services, followed by **East Java** and **West Java** as **medium**-risk regions. All 30 other regions are **low** risk.

Jakarta and **Riau Islands** recorded the highest values of risk compared with other regions. The respective positions on the y-axis of the heatmap show that the consequence of terrorist financing in non-bank Money or Value Transfer Services located in the provinces of Jakarta and Riau Islands is the highest of all provinces.

The high threat and consequence scores of Jakarta and Riau Islands were influenced by the high number of suspicious transaction reports from 2019-2020 in both provinces. As an economic, business and government centre, most business activity and transactions are conducted in Jakarta. Meanwhile, regions with geographical proximity to international borders and different jurisdictions, such as the Riau Islands, demand vigilance in terms of terrorist financing risk mitigation efforts.

The provinces of **East Java** and **West Java** received a higher threat score than other provinces, coupled with medium vulnerability and consequence scores. Large cities, as centres of economic activity and growth, provide terrorist groups access to funding transactions through legal businesses and financial services providers. Furthermore, there is a high number of service points for non-bank Money or Value Transfer Services in such regions, offering access to transactions that facilitate the collection, transfer and use of terrorist financing.

According to the FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services published in 2016, no universal definition or methodology has been put forward to determine which countries or geographical locations are high-risk in terms of terrorist financing. Notwithstanding, a range of factors may indicate risk as follows:

a. Countries or jurisdictions identified by credible sources, namely reputable and universally recognised international organisations, as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

b. Countries subject to sanctions, embargoes or similar measures issued by international organisations, such as the United Nations.

c. Countries identified as having weak law enforcement and regulatory regimes, including countries identified by FATF Statements as having weak AML/CFT regimes based on credible independent sources, such as FATF, APG, CFATF, MONEYVAL, OECD, etc.

d. Countries identified as having weak governance, as determined by the World Bank.

e. Countries or areas identified as having significant levels of corruption, narcotics (including source or transit countries for illegal drugs), human trafficking and/or illicit trafficking in protected animal species, and illegal gambling based on the latest credible and independent sources.

2. Terrorist Financing Risk based on Individual Customer Profile

Terrorist financing risk was also assessed based on individual customer profile to ascertain which individuals (professions) and corporations (business entities) were most at risk to terrorist financing via non-bank Money or Value Transfer Services. The customer profiles used in this risk assessment refer to those applied in the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021. Terrorist financing risk based on individual customer profile in non-bank Money or Value Transfer Services was assessed based on the following limitations:

a. The obligations of non-bank Money or Value Transfer Services to administrate customer information in accordance with Article 51, Paragraph (1) of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Implementation of Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) for Payment Service Providers and Non-Bank Money Changers.

b. The dominance of walk-in customers at non-bank Money or Value Transfer Services.

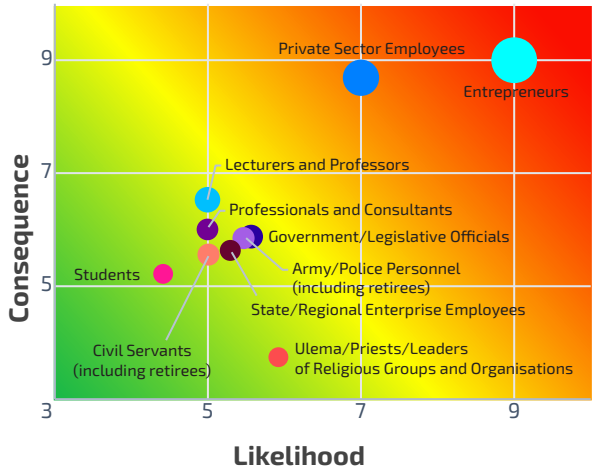
Risk scores for different customer profiles were calculated by multiplying the likelihood and consequence scores for each customer profile, while the likelihood was obtained by adding the threat and vulnerability scores. The results of the risk analysis of terrorist financing in non-bank Money or Value Transfer Services based on risk by customer profile are recapitulated in Table 3.8.

Table 3.8. Risk Analysis of Terrorist Financing in Non-Bank Money or Value Transfer Services by Individual Customer Profile

No	Profile	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Entrepreneurs	9.00	6.69	9.00	9.00	9.00	High
2.	Private Sector Employees	7.38	5.04	8.63	6.98	6.93	Medium
3.	Lecturers and Professors	3.83	5.39	6.53	4.99	4.96	Low
4.	Government/Legislative Officials	4.14	6.00	5.77	5.56	4.92	Low
5.	Army/Police Personnel (including retirees)	4.19	5.79	5.74	5.47	4.86	Low
6.	Professionals and Consultants	3.96	5.26	5.92	4.99	4.71	Low
7.	State/Regional Enterprise Employees	3.07	6.63	5.49	5.29	4.67	Low
8.	Civil Servants (including retirees)	4.97	4.28	5.40	5.01	4.50	Low
9.	Student	4.63	3.71	5.26	4.45	4.19	Low
10.	Others	3.55	4.54	3.73	4.29	3.57	Low

The results of mapping terrorist financing risk in non-bank Money or Value Transfer Services by individual customer profile is presented in Figure 3.7

Figure 3.7. TF Risk Heatmap by Individual Customer Profile in MVTS Sector



According to the TF risk heatmap presented in Figure 3.7, **Entrepreneurs** are **high** risk for terrorist financing in non-bank Money or Value Transfer Services, while **Private Sector Employees** are **medium**-risk customer profiles.

Entrepreneurs recorded the highest scores in terms of threat and consequence, followed by **Private Sector Employees** with higher threat and consequence scores than the other customer profiles. **Entrepreneurs** represent the customer profile most frequently appearing in Suspicious Transaction Reports (LKTM) and Cash Transaction Reports (TKT) from 2019-2022. Furthermore, the results of a survey also showed that customers of non-bank Money or Value Transfer Services are dominated by Entrepreneurs and Private Sector Employees.

A White Paper published in 2017 found that self-funding was used by terrorist groups. In addition, most customers of non-bank Money or Value Transfer Services are Entrepreneurs and Private Sector Employees. Private Sector Employees received medium vulnerability and consequence scores due to the high number and value of suspicious transactions and cash transactions via non-bank Money or Value Transfer Services.

According to the FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services published in 2016, the following activities may indicate a high risk of terrorist financing:

a. Customer is another Non-Bank Money or Value Transfer Services or Payment Service Provider that has been sanctioned by the respective national competent authority for its non-compliance with the AMF/CFT applicable regime.

b. Customer conducting their business relationship or transactions in unusual circumstances, such as:

   1. Customer who travels unexplained distances to locations to conduct transactions.

   2. Defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services.

   3. Customer owns or operates a cash-based business that appears to be a front or shell company or is mingling illicit and illicit proceeds as determined from a review of transactions that seem inconsistent with the financial standing or business profile.

c. Politically Exposed Persons (PEP)[32] or his/her family members or close associates.

d. Non-face-to-face customer, where doubts exist about the identity of such a customer.

e. Customer who uses agents or associates where the nature of the relationship or transaction makes it difficult to identify the beneficial owner of the funds.

f. Customer knows little or is reluctant to disclose details about the payee (contact information, address and other information).

g. Consumer gives inconsistent information, such as providing different names.

h. Customer involved in the transactions that has no apparent ties to the destination country and with no reasonable explanation.

i. Suspicion that the customer is acting on behalf of a third party but not disclosing that information or is being controlled by someone else. For example, the customer picks up a money transfer and immediately hands it to someone else.

j. Customer has been the subject of law enforcement sanctions.

k. Customer offers false/fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents.

l. Customer whose transactions and activities indicates connection with potential criminal involvement, typologies or red flags provided in reports produced by the FATF or Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

m. Customer whose transaction patterns appear consistent with the generation of criminal proceeds, for example, illegal drug growing season, period of immigrant worker departures, corruption, based on information available with the MVTS.

Consistent with the findings of the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021, the latest findings show the emerging threat of using immediate family members, such and spouses and children, and well as other parties, to transfer funds to finance terrorists in order to avoid the List of Suspected Terrorists and Terrorist Organisations (DTTOT). Based on the FATF Guidance on Terrorist Financing Risk Assessment published in 2019, terrorist groups are known to utilise local diaspora populations, communities as well as ethnic and family ties to collect and transfer funds and other assets to support terrorist activity.

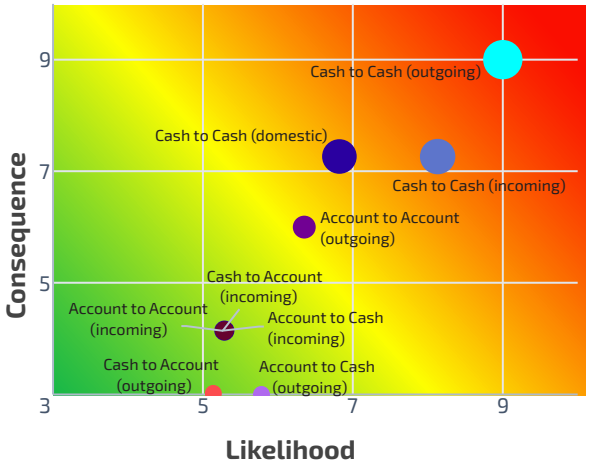
3. Terrorist Financing Risk based on Products

32 According to FATF Guidance on PEP, politically exposed persons (PEP), including individuals who are or have been entrusted with a public or prominent function, are high-risk customer profiles. In the context of individual customer profiles, Government/Legislative Officials, State/Regional Enterprise Employees (including retirees), Civil Servants (including retirees), Army/Police Personnel (including retirees), Lecturers and Professors serving as University Rectors as well as Political Party Leaders are domestic PEPs.

and Services

Terrorist Financing risk was also assessed based on the products and services to ascertain which were most at risk to cases of terrorist financing in non-bank Money or Value Transfer Services. The products of non-bank Money or Value Transfer Services are outgoing transfers (from Indonesia), incoming transfers (to Indonesia) and domestic transfers (within Indonesia). In addition, money transfer mechanisms include cash to cash, cash to account, account to cash and account to account. In total, therefore, 12 products and services of non-bank Money or Value Transfer Services were assessed in terms of money laundering risk. Risk scores for the products and services of non-bank Money or Value Transfer Services were calculated by multiplying the likelihood and consequence for each product or service, while the likelihood was obtained by adding the threat and vulnerability. The results of terrorist financing risk analysis in non-bank Money or Value Transfer Services based on products and services using several risk factors in the form of risk are presented in Table 3.9.

Figure 3.8. TF Risk Heatmap by Product and Service in MVTS Sector



The results of mapping terrorist financing risk in non-bank Money or Value Transfer Services by product and service is presented in Figure 3.8.

According to the TF risk heatmap presented in Figure 3.8, **Cash to Cash (outgoing, incoming, domestic)** is considered a **high**-risk product for terrorist financing in non-bank Money or Value Transfer Services, while **Account to Account (outgoing)** is **medium** risk.

Table 3.9. Risk Analysis of Terrorist Financing in MVTS Sector by Product and Service

No	Product and Service	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Cash to Cash (Outgoing)	9.00	5.50	9.00	9.00	**9.00**	High
2.	Cash to Cash (Incoming)	8.35	5.00	7.32	8.08	**8.01**	High
3.	Cash to Cash (Domestic)	6.79	5.00	7.29	6.84	**7.46**	High
4.	Account to Account (Outgoing)	6.47	4.50	6.00	6.18	**5.42**	Medium
5.	Account to Cash (Incoming)	5.83	4.00	4.32	5.26	**4.52**	Low
6.	Cast to Account (Incoming)	5.83	4.00	4.32	5.26	**4.22**	Low
7.	Cash to Account (Outgoing)	5.21	4.50	3.00	5.16	**4.21**	Low
8.	Account to Account (Incoming)	5.83	4.00	4.32	5.26	**4.19**	Low
9.	Account to Cash (Outgoing)	6.47	4.00	3.00	5.78	**4.10**	Low
10.	Account to Cash (Domestic)	4.26	4.00	4.29	4.01	**4.06**	Low
11.	Cash to Account (Domestic)	4.26	4.00	4.29	4.01	**3.82**	Low
12.	Others	3.00	4.00	4.29	3.00	**3.00**	Low

Cash to Cash (outgoing, incoming, domestic) recorded the highest values of threat and consequence compared with the other products. The position of Cash to Cash on the x-axis of the TF heatmap shows the highest likelihood compared with the other products, while the position on the y-axis shows the highest consequence if the product is misused for terrorist financing through non-bank Money or Value Transfer Services.

The high frequency and value of Suspicious Transaction Reports (LKTM) for Cash to Cash and Account to Account (outgoing) products from 2019-2020 also contributed to the high threat and consequence scores for these products. Consistent with the findings of the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021, the use of cash transactions remains the conventional method predominantly used by terrorist groups because cash transactions are convenient, safe and difficult to trace and track.

According to the FATF Guidance for a Risk-Based Approach: Money or Value Transfer Services[33] published in 2016, the following products and services may indicate a high risk of money laundering:

a. Products or services that may inherently favour anonymity or products that can readily cross international borders, such as cash and online money orders, to beneficiaries with unverified identities.

b. Products or services that have a very high transaction limit.

c. Products and services with global reach.

d. Complex products and services.

e. Products and services that permit the exchange of cash for a negotiable instrument, such as a money order or chip-based electronic money.

Notwithstanding, based on the Sectoral Risk Assessment using a sample of non-bank Money or Value Transfer Services, most licensed non-bank Money or Value Transfer Services are implementing effective AML/CFT policy for all products and services.

4. Terrorist Financing Risk based on Delivery Channel

Terrorist financing risk was also assessed based on the delivery channel to ascertain which were most at risk to cases of terrorist financing in non-bank Money or Value Transfer Services. The delivery channels as objects of this risk assessment are grouped into three main categories, namely the offices of non-bank Money or Value Transfer Services, Agents and Mobile Applications. Terrorist financing risk based on delivery channel in the MVTS sector was assessed by multiplying the level of likelihood and consequence for each delivery channel, while the likelihood was obtained by adding the threat and vulnerability. Using risk factors in the form of risk, the level of terrorist financing risk for each delivery channel in the MVTS sector was assessed and the results are presented in Table 3.10.

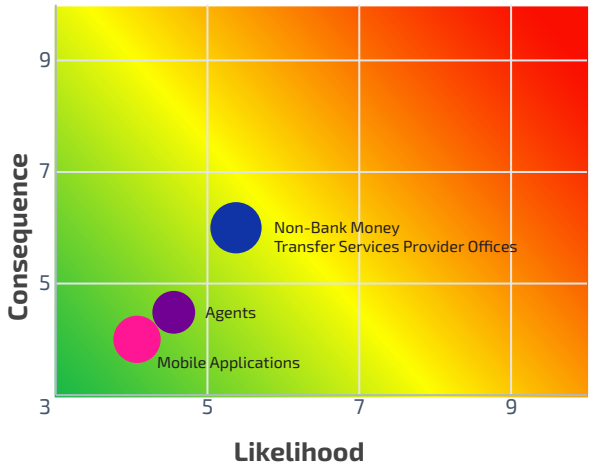
33 https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

Table 3.10. Risk Analysis of Terrorist Financing in Non-Bank Money or Value Transfer Services by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-Bank Money or Value Transfer Services	5.50	5.25	6.00	5.38	**5.01**	Medium
2.	Mobile Applications	4.00	4.14	4.00	4.07	**4.43**	Low
3.	Agents	5.00	4.11	4.50	4.56	**4.28**	Low

The results of mapping terrorist financing risk in non-bank Money or Value Transfer Services by delivery channel is presented in Figure 3.9.

Figure 3.9. TF Risk Heatmap by Delivery Channel in MVTS Sector



According to the TF risk heatmap presented in Figure 3.9, no delivery channels of non-bank Money or Value Transfer Services are considered **high**-risk for terrorist financing. Notwithstanding, the **Offices of Non-Bank Money or Value Transfer Services** are a **medium**-risk delivery channel, while **Agents** and **Mobile Applications** are **low** risk.

According to the FATF Guidance on Terrorist Financing Risk Assessment published in 2019, terrorist groups are known to use different channels move funds and assets, including through the banking sector, money service businesses (MSB), cash smuggling, informal remittances, etc.

In the context of terrorist financing, there were no court reports or cases involving non-bank Money or Value Transfer Services from 2019-2020. Nevertheless, the offices of non-bank Money or Value Transfer Services received a higher threat score than the other delivery channels due to the broad office network that is used extensively. Consistent with the outcome of the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021, one of the typologies found was the use of private sponsors (terrorist financiers), thus exposing the offices of non-bank Money or Value Transfer Services as a channel that can be exploited to finance terrorists.

3

RISK MITIGATION

A. Institutional Aspects of Risk Mitigation

1. Non-bank Money or Value Transfer Services in Indonesia must be licensed by Bank Indonesia.
2. Non-bank Money or Value Transfer Services must be legally incorporated as business entities in Indonesia.
3. At least 15% of the shareholdings of non-bank Money or Value Transfer Services must be owned by Indonesian citizens and/or Indonesian business entities, and at least 51% of the shares with voting rights must be owned by Indonesian citizens and/or Indonesian business entities.
4. Licence applications must be accompanied by documents and/or other requirements in the form of documents relating to the institutional and financial conditions as well as documents relating to operational readiness.
5. Directors and owners of non-bank Money or Value Transfer Services must meet the following requirements stipulated by Bank Indonesia:
    a. Never been declared bankrupt or a director or member of board of commissioners of a company declared bankrupt within a period of five years prior to the date of application.
    b. Never been convicted of a banking or financial crime and/or money laundering based on a court verdict with permanent legal force.
    c. Not included on the blacklist of bad debt at the time of submitting the application.
    d. Not included on the National Blacklist (DHN) for withdrawals of blank cheques and/or money transfers.
6. Bank Indonesia may determine the validity period of a PJP licence as required based on licence category, business activity and/or the source of funding.
7. Bank Indonesia evaluates the PJP licence every three years or as required.
8. Licensed non-bank Money or Value Transfer Services are prohibited from transacting with unlicensed or illegal non-bank Money or Value Transfer Services.

B. Operational Aspects of Risk Mitigation

a. Pre-Transaction Mitigation Measures

1. Directors and Board of Commissioners supervise AML/CFT program implementation.
2. Non-bank Money or Value Transfer Services implement employee screening, customer due diligence and employee capacity building.
3. Non-bank Money or Value Transfer Services implement robust internal control measures, including regular independent audits, to test AML/CFT implementation compliance and effectiveness.
4. Non-bank Money or Value Transfer Services identify, assess, control and mitigate risk.
5. Non-bank Money or Value Transfer Services subscribe to the databases of competent authorities, such as the Directorate General of Population and Civil Registration of Indonesia and PEP database developed by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), to assist the customer identification and verification process.

b. Transaction Mitigation Measures

1. Non-bank Money or Value Transfer Services implement enhanced due diligence for high-risk prospective customers, customers and beneficial owners.
2. Non-bank Money or Value Transfer Services utilise information technology to support the application of Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) procedures, including electronic Know Your Customer (e-KYC). Information

technology also includes liveness detection for face recognition and biometric verification.

3. Non-bank Money or Value Transfer Services apply Regulatory Technology (RegTech) in the implementation of risk-based Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT).
4. Non-bank Money or Value Transfer Services identify and red flag unusual transaction patterns.

c. Post-Transaction Mitigation Measures

1. Non-bank Money or Value Transfer Services implement ongoing customer due diligence regarding money transfer patterns and amounts.
2. Non-bank Money or Value Transfer Services identify and report suspicious transactions to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).
3. Non-bank Money or Value Transfer Services implement identification and verification procedures, data, information and document management as well as reporting to competent authorities.

d. Additional Risk Mitigation Measures Relating to Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction:

1. Non-bank Money or Value Transfer Services block or freeze funds belonging to individuals or corporations identified on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).
2. Non-bank Money or Value Transfer Services conduct rigorous investigations concerning the modus operandi and typologies of terrorist financing cases used by terrorist groups for more effective preventative measures.
3. Non-bank Money or Value Transfer Services administrate and update the List of Proliferation Financing as well as the FATF List of High-Risk Jurisdictions Subject to a Call for Action and Jurisdictions Under Increased Monitoring based on automatic screening to mitigate proliferation financing of weapons of mass destruction.
4. Non-bank Money or Value Transfer Services subscribe to international databases, such as World-Check, in relation to Politically Exposed Persons (PEP) and the List of Suspected Terrorists and Terrorist Organisations (DTTOT) and List of Proliferation Financing in order to mitigate terrorist financing and financing of proliferation of weapons of mass destruction.
5. Non-bank Money or Value Transfer Services implement enhanced due diligence for high-risk prospective customers, customers or beneficial owners to mitigate the exploitation of immediate family members, including wives, children and others, to finance terrorism.
6. In terms of collaborating with third parties, such as agents or partners, non-bank Money or Value Transfer Services ensure adequate AML/CFT implementation by the third party, including money transfers to and from Indonesia indicated for terrorism, terrorists and terrorist organisations.

C. Supervision Aspects of Risk Mitigation

1. Bank Indonesia conducts direct and indirect risk-based supervision in relation to AML/CFT implementation by non-bank Money or Value Transfer Services.
2. Bank Indonesia performs thematic supervision of non-bank Money or Value Transfer Services.
3. Bank Indonesia may assign other parties for and on behalf of Bank Indonesia to perform inspections of non-bank Money or Value Transfer Services.
4. For Bank Indonesia supervision, non-bank Money or Value Transfer Services must identify, manage and update data concerning the Beneficial Owners, while ensuring the availability of data on Beneficial Owners in the interest of Bank Indonesia supervision.

4

CONCLUSIONS

A. Money Laundering Risks

Based on the outcome of statistical data analysis and the risk score of sectoral money laundering in non-bank Money or Value Transfer Services by **region (province), customer profile, product** and **service** as well as **delivery channel**, the following conclusions were drawn:

1. The **Special Capital Region of Jakarta** is a **high-risk** region concerning money laundering activity in non-bank Money or Value Transfer Services, followed by the provinces of **West Java, Riau Islands, East Java** and **Central Java** as **medium-risk** regions. All other provinces are **low** risk.

2. **Entrepreneurs, Private Sector Employees** and **Politically Exposed Persons (PEP)** are **high-risk** individual customer profiles for money laundering activity in non-bank Money or Value Transfer Services, followed **Housewives, Professionals** and **Consultants** as **medium** risk. All other individual customer profiles are **low** risk.

3. **Non-MSME Limited Liability Companies (PT)** are **high-risk** institutional customer profiles for money laundering activity in non-bank Money or Value Transfer Services, followed by **Government Institutions** as **medium** risk. All other institutional customer profiles are **low** risk.

4. **Cash to Account (outgoing)** is considered a **high-risk** product for money laundering activity in non-bank Money or Value Transfer Services, followed by **Account to Account (incoming)** as **medium** risk. All other products and services of non-bank Money or Value Transfer Services are **low** risk.

5. **Non-bank Money or Value Transfer Services** are a **medium-risk** delivery channel for money laundering activity in non-bank Money or Value Transfer Services, followed by **Agents** and **Mobile Applications** as **low**-risk delivery channels.

Table 3.11. Outcome of Sectoral Risk Assessment of Money Laundering in MVTS Sector

Risk	Province	Profession	Business Entity	Product/Service	Delivery Channel
High	Jakarta	Entrepreneurs, Private Sector Employees , and PEP	Non-MSME Limited Liability Companies (PT)	Cash to Account (Outgoing)	-
Medium	West Java, Riau Island, East Java, Central Java	Housewives, Profesional dan Konsultaan	Government Institutions	Account to Account (Incoming)	Non-bank Money or Value Transfer Services
Low	Others	Others	Others	Others	Mobile Applications, Agents

B. Terrorist Financing Risk

Based on the latest assessment, the level of terrorist financing risk in non-bank Money or Value Transfer Services is as follows:

1. The **Special Capital Region of Jakarta** and **Riau Islands** are **high-risk** regions for terrorist financing activity in non-bank Money or Value Transfer Services, followed by the provinces of **West Java** and **East Java** as **medium-risk** regions. All other provinces are **low** risk.

2. **Entrepreneurs** are a **high-risk** individual customer profile for terrorist financing activity in non-bank Money or Value Transfer Services, followed **Private Sector Employees** as **medium** risk. All other individual customer profiles are **low** risk.

3. **Cash to Cash (outgoing, incoming, domestic)** is a **high-risk** product for terrorist financing activity in non-bank Money or Value Transfer Services, followed by **Account to Account (outgoing)** as **medium** risk. All other products and services are **low** risk.

4. No delivery channels of non-bank Money or Value Transfer Services are **high** risk for terrorist financing. Notwithstanding, the **Offices of Non-Bank Money or Value Transfer Services** are a **medium-risk** delivery channel, while **Agents** and **Mobile Applications** are **low** risk.

Table 3.12. Outcome of Sectoral Risk Assessment of Terrorist Financing in MVTS Sector

Risk	Province	Profession	Product/Services	Delivery Channel
High	Jakarta, Riau Island	Entrepreneurs	Cash to Cash (Outgoing, Incoming, Domestic)	-
Medium	West Java, East Java	Private Sector Employees	Account to Account (Outgoing)	Non-bank Money or Value Transfer Services
Low	Others	Others	Others	Mobile Application, Agents

PART II

NON-BANK ELECTRONIC MONEY ISSUERS AND NON-BANK ELECTRONIC WALLET SERVICE PROVIDERS


Rp
CreditCard
Rp
Rp
Rp

EXECUTIVE SUMMARY

In 2021, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), in conjunction with relevant government ministries/ agencies, identified, analysed and evaluated the latest money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks holistically through the national risk assessment program, namely the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021. Based on the NRA of Money Laundering 2021, Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers are considered a low-risk industry. Notwithstanding, as a follow-up action to mitigate the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank electronic money issuers and non-bank electronic wallet service providers, a sectoral risk assessment (SRA) of money laundering, terrorist financing and proliferation financing of WMD was performed covering non-bank electronic money issuers and non-bank electronic wallet service providers with the following objectives:

1. Identifying and analysing the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank electronic money issuers and non-bank electronic wallet service providers.

2. Identifying, analysing and evaluating various risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction based on risk mapping the **customer profiles (individual and corporate), regions (provinces), products and services** as well as **delivery channels** of non-bank electronic money issuers and non-bank electronic wallet service providers.

3. Identifying and analysing the emerging threats of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank electronic money issuers and non-bank electronic wallet service providers.

4. Formulating strategic risk mitigation measures against money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank electronic money issuers and non-bank electronic wallet service providers.

The SRA of money laundering and terrorist financing in non-bank electronic money issuers and non-bank electronic wallet service providers mapped four key risks based on customer profile, region, product and service as well as delivery channel and formulated risk factors covering the threats, vulnerabilities and consequences. The analysis methodology referred to the risk assessment method issued by the Financial Action Task Force (FATF). According to the latest assessment, the level of money laundering risk in non-bank Money or Value Transfer Services is as follows:

1. The **Special Capital Region of Jakarta** is a **high-risk** region concerning money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers, followed by the provinces of **West Java, East Java** and **North Sumatra** as **medium-risk** regions. All other provinces are **low** risk.

2. **Non-MSME Limited Liability Companies (PT)** and **Government Institutions (including state/regional-owned enterprises)** are considered **medium-risk** institutional customer profiles for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other institutional customer profiles are **low** risk.

3. **Private Sector Employees, Politically Exposed Persons (PEP)** and **Students** are **high-risk** individual customer profiles for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers, followed **Entrepreneurs** and **Housewives** as **medium** risk. All other individual customer profiles are **low** risk.

4. **Purchase & Payment** is a **high-risk** product for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers, followed by **Cashless Top Up** as **medium** risk. All other products and services of non-bank electronic money issuers and non-bank electronic wallet service providers are **low** risk.

5. **Offline Merchants, Mobile Applications** and **Online Merchants** are **medium-risk** delivery channels for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other delivery channels are **low** risk.

Based on the latest assessment, the level of terrorist financing risk in non-bank electronic money issuers and non-bank electronic wallet service providers is as follows:

1. The **Special Capital Region of Jakarta** and **West Java** are **medium-risk** regions for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other provinces are **low** risk.

2. **Entrepreneurs** and **Students** are **medium-risk** individual customer profiles for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other individual customer profiles are **low** risk.

3. **Purchase & Payment** and **Money Transfers** are **medium-risk** products for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other products and services are **low** risk.

4. **Online Merchants** are a **medium-risk** delivery channel for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other delivery channels are **low** risk.

There have been no significant cases relating to proliferation financing of WMD identified in Indonesia but the potential risks must still be anticipated. Bank Indonesia has issued regulations and guidelines as well as performed direct and indirect supervision to mitigate the risks associated with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank electronic money issuers and non-bank electronic wallet service providers. Furthermore, Bank Indonesia actively cooperates domestically and internationally. Meanwhile, Bank Indonesia has also organised socialisation and education activities targeting non-bank electronic money issuers and non-bank electronic wallet service providers and members of the public to increase awareness of the risks and support efforts to prevent and eradicate money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

1

LITERATURE REVIEW OF NON-BANK ELECTRONIC MONEY ISSUERS AND NON-BANK ELECTRONIC WALLET SERVICE PROVIDERS

A. Legal Basis

Bank Indonesia is a supervisory and regulatory body (LPP) for non-bank electronic money issuers and non-bank electronic wallet service providers in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (ML Act) as well as Act No. 9 of 2013 concerning the Prevention and Eradication of Terrorist Financing (TF Act). Regulations specific to non-bank electronic money issuers are contained in Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, while regulations pertaining to non-bank electronic wallet service providers are contained in Bank Indonesia Regulation (PBI) No. 18/14/PBI/2016 concerning Payments Transaction Processing. The salient provisions of the PBI on Electronic Money cover the following:

1. Principles and scope of electronic money.
2. Licensing and approval of electronic money.
3. Application of risk management.
4. Information systems security standards.
5. Application of anti-money laundering and combating the financing of terrorism (AML/CFT).
6. Application of consumer protection principles.
7. Implementation of digital financial services (DFS).
8. Reporting and supervision.
9. Sanctions.

Since July 2021, however, regulations concerning the payment system are in accordance with Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System (PBI PS) as well as Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning Payment Service Providers (PJP) and Bank Indonesia Regulation (PBI) No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PIP). Based on the latest payment system regulations, electronic money and electronic wallets are data storage instruments and services that can initiate payment transactions and/or provide access to sources of funds for payment. Furthermore, non-bank payment service providers that administrate sources of funds in the form of issuing electronic money can offer top up features, retail transaction payments, utility bill payments, money transfers and cash out as well as other features based on approval by Bank Indonesia. Provisions contained within the Bank Indonesia regulation on Payment Service Providers pertaining to the administration and issuance of electronic money are as follows:

1. Obligations to apply risk management and consumer protection principles, including transaction caps, limits on the value of electronic money store, limits on cash withdrawals and limits on access to other sources of funds as determined by Bank Indonesia.

2. Reporting obligations to Bank Indonesia concerning the planned implementation and completion of trials to test the readiness of PJP activities in the licensing process.

3. Obligations to maintain appropriate systems and mechanisms that record and monitor availability as well as maintain a Floating Fund in accordance with prevailing regulations.

4. Obligations to apply strict security standards for electronic money transactions exceeding Rp2 million using two factor authentication or other security standards set by Bank Indonesia.

5. Obligations to limit requests and use of data and/or information regarding electronic money users, provide top-up facilities and/or infrastructure as well as maintain mechanisms for financial compensation to electronic money uses in the interest of consumer protection.

6. Obligations to obtain approval from Bank Indonesia before developing or expanding activities, products and/or cooperation, and before offering digital financial services (DFS).

7. Obligations to cooperate with bank payment service providers (PJP) and connect to the national payment gateway or the interconnection and interoperability mechanism determined by Bank Indonesia for parties conducting electronic money transactions issued outside the territory of Indonesia.

B. Characteristics of Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers in Indonesia

1. Definition

Electronic Money[34] is defined as a payment instrument meeting the following criteria

a. Issued based on the value of money paid in advance to an issuer.

b. The value of money stored electronically on a server or chip.

An issuer is a party issuing electronic money, while the value of electronic money is the value stored electronically on a server or chip which can be transferred for payment transactions and/or money transfers. The value of electronic money managed by an issuer is not defined as a deposit in accordance with laws regulating the banking industry. Any party wishing to act as a payment service provider must be licensed by Bank Indonesia[35]. Licences are granted to payment service providers based on the licence category without a predetermined validity period. Payment service providers (PJP) as issuers of electronic money are required to apply Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) principles as well as consumer protection principles.

Service providers are required to process electronic money transactions domestically for payment transactions using electronic money issued and transacted in the territory of the Republic of Indonesia. Electronic money issued outside the territory of Indonesia can only be transacted within the territory of Indonesia using a payment channel connected to the national payment gateway. Transacting parties are required to cooperate with a licensed payment service provider, namely a BUKU 4[36] category commercial bank that is connected to the national payment gateway. Bank Indonesia conducts fit and proper tests on the controlling shareholders, board of directors and board of commissioners of non-bank institutions.

2. Products and Services

Electronic money is classified as follows:

a. Based on the scope of implementation, either closed-loop[37] or open-loop[38]

34 Article 156 of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning payment service providers.

35 Article 11 of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers.

36 In accordance with Bank Indonesia Regulation (PBI) No. 14/26/PBI/2012 concerning Bank Business Activity and Office Networks based on Core Capital, BUKU 4 banks must maintain a core capital exceeding Rp30 trillion.

37 In accordance with Article 158, letter (a) of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers, closed loop is Electronic Money which may only be used as a payment instrument to a goods and/or service provider which is also the Issuer of the Electronic Money.

38 In accordance with Article 158, letter (b) of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers, open loop is Electronic Money which may be used as a payment instrument to a goods and/or service provider which is not the Issuer of the Electronic Money.

electronic money.

b. Based on the storage medium, either server-based[39] or chip-based[40] electronic money.

c. Based on the recording of a customer's identity data, either registered[41] or unregistered[42] electronic money.

Any party acting as a Provider in the form of a closed-loop issuer with a floating fund of less than Rp1 billion is not required to obtain a licence from Bank Indonesia. The limit on unregistered electronic money which may be stored is Rp2 million and Rp10 million for registered electronic money, with transactions limited to Rp20 million per month based on incoming transactions.

In accordance with the Bank Indonesia regulation on payment service providers, the electronic money features which may be provided by the issuer consist of the following:

a. Cash and/or cashless top up.

b. Payment of retail transactions and/or payment of utility bills.

c. Money transfers and cash out for open-loop electronic money and registered customers.

39 In accordance with Article 159, letter (a), point (1) of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers, server-based is Electronic Money stored on a server.

40 In accordance with Article 159, letter (a), point (2) of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers, chip-based is Electronic Money stored on a chip.

41 In accordance with Article 159, letter (b), point (1) of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers, registered is Electronic Money for which the customer's identity data is registered and recorded with the Issuer.

42 In accordance with Article 159, letter (b), point (2) of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers, unregistered is Electronic Money for which the customer's identity data is not registered and not recorded with the Issuer.

According to the latest payment system regulations, platform providers with an active user base totalling or expected to reach 300,000 customers must first obtain a licence from Bank Indonesia[43].

3. Delivery Channels

The delivery channels of non-bank electronic money issuers and non-bank electronic wallet service providers can be divided into two categories, namely to process the registration of service users (customers) as well as to use the products and services of non-bank electronic money issuers and non-bank electronic wallet service providers. The registration process for service users is performed through a mobile application or outlet and/or DFS agent. Meanwhile, to use purchase & payment products and services, the delivery channels are offline merchants and online merchants. Service users can use cash and cashless top up features and transfer funds between banks (ATM/debit cards and/or mobile/SMS/internet banking) and/or agents of non-bank electronic money issuers and non-bank electronic wallet service providers and mobile applications.

4. Providers

As of 31st May 2021, a total of 41 non-bank institutions were licensed as non-bank electronic money issuers and six non-bank electronic wallet service providers. Based on distribution data for non-bank electronic money issuers and non-bank electronic wallet service providers, 37 issuers are located in the Special Capital Region of Jakarta and four issuers are located in the provinces of Banten, West Java and East Java. According to Bank Indonesia data, most payment service providers licensed as non-bank electronic wallet service providers are also licensed as non-bank electronic money issuers, thus the risk assessment of both instruments was consolidated.

43 In accordance with Article 198 of Bank Indonesia Regulation (PBI) No. 23/6/PBI/2011 concerning Payment Service Providers.

2

KEY RISKS IN NON-BANK ELECTRONIC MONEY ISSUERS AND NON-BANK ELECTRONIC WALLET SERVICE PROVIDERS

A. Money Laundering Risk Landscape

The typologies of money laundering have evolved in Indonesia over time to become more complex and varied by exploiting financial system institutions. Technological advancement in the financial system, which has transformed into a digital payment system, including non-bank electronic money issuers and non-bank electronic wallet service providers, is also being exploited by criminals. The potential for money laundering via non-bank electronic money issuers and non-bank electronic wallet service providers as an additional payment instrument is increasing in line with the growing number of customers and volume of electronic money transactions. Furthermore, the Covid-19 pandemic has precipitated a paradigm shift as members of the public accept and prefer to use electronic money as a payment instrument. According to Bank Indonesia, transaction value using electronic money reached Rp27.6 trillion in September 2021, up 56.3% on September 2020. Based on the National Risk Assessment (NRA) of Money Laundering, growth of electronic money and electronic wallets as payment instruments via e-commerce represents another challenge as criminals exploit e-commerce to funnel illicit proceeds of crime. In the third quarter of 2021, Bank Indonesia data showed that e-commerce payment transactions were dominated by electronic money in terms of value (39.8%) and volume (30.07%), placing second after bank transfers.

According to the Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services published by FATF in 2013, the following risk factors of money laundering and terrorist financing were identified using electronic payment instruments:

1. Customer Due Diligence: Electronic payment instruments contain risk if the customer's identification is not verified by an independent and credible source given the non-face-to-face nature of transactions that are vulnerable to the use of false identification documents or the identification documents of another person.

2. Record Keeping: The risk of money laundering and terrorist financing increases at issuers without proper record keeping because the recording of electronic transaction data plays an important role in the criminal investigation process.

3. Value limits: The application of maximum limits on the amount stored, transaction value and number of transactions can reduce the risk of using electronic payment instruments by perpetrators of money laundering and terrorist financing.

4. Top Up: Anonymous funding sources that are difficult to detect influence the level of risk in electronic payment instruments.

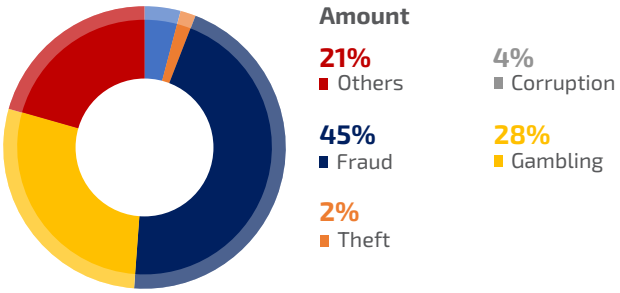
5. Geographical Limits: Electronic payment instruments that can be used across national and regional borders influence the level of risk in electronic payment instruments.

6. Usage Limits: More features and/or flexibility when using electronic payment instruments increases the risk such instruments can be misused for money laundering and terrorist financing.

7. Segmentation of Services: The segmentation of services involving outsourcing to third parties influences the level of risk in electronic payment instruments.

Though no significant cases of money laundering typologies have been discovered in Indonesia using non-bank electronic money issuers and non-bank electronic wallet service providers, perpetrators of predicate crimes could use the features offered by electronic money and electronic wallets to commit money laundering offences. Data from Suspicious Transaction Reports (STR) from 2019-2020 showed that predicate offences using electronic money and electronic wallets for money laundering were dominated by theft and gambling.

Graph 4.1. Composition of Predicate Offences based on Suspicious Transaction Reports in Non-Bank EM and EW



Source: Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)

Based on data from the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) and the FATF Report on Money Laundering Using New Payment Methods and APG Yearly Typologies Report, the following money laundering typologies using non-bank electronic money issuers and non-bank electronic wallet service providers were identified:

1. Using false identification documents or the identification documents of someone else to open/register and electronic money/electronic wallet account to conceal the identity of the Beneficial Owner.

2. Purchasing and/or using the electronic money/ electronic wallet account of someone else to conceal the identity of the Beneficial Owner.

3. Using an electronic money account as a repository for the illegal proceeds of crime.

4. Using cash to top up an account to conceal the identity of the sender and origin of the source of funds.

5. Using money transfer and/or cash out features to transfer electronic money balances obtained from the illicit proceeds of crime.

6. Identity theft to link credit cards or debit cards to the electronic money/electronic wallet account of a criminal. The perpetrator subsequently uses the stolen credit cards or debit cards as a source of funds for transactions.

7. Failing to repay post-paid funds.

8. High-frequency transactions of relatively small value during a given period (structuring).

9. Transactions using several electronic money and electronic wallet accounts (smurfing).

10. Using purchase & payment features where the seller and buyer conspire to create fictitious transactions for trade-based money laundering.

11. Use of money mules/straw accounts.

12. Incoming transactions followed by cash out transactions.

13. Incoming transactions from various parties at the same time.

B. Terrorist Financing Risk Landscape

Based on the FATF report on Emerging Terrorist Financing Risks published in 2015, terrorist financing typologies are becoming more varied over time and with new technologies. Though no significant cases of money laundering have been discovered in Indonesia using non-bank electronic money issuers and non-bank electronic wallet service providers, emerging threats of terrorist financing using electronic money and electronic wallets are increasing in line with the growing number of customers and volume of electronic money transactions. Perpetrators of terrorist financing can exploit the features offered by electronic money and electronic wallets as a media to collect, transfer and utilise funds.

Based on the FATF reports on Money Laundering Using New Payment Methods and Emerging Terrorist Financing Risks published in 2010 and 2015 respectively, as well as the APG Yearly Typologies Report, the following terrorist financing typologies exploiting non-bank electronic money issuers and non-bank electronic wallet service providers have been identified:

1. Using false identification documents or the identification documents of someone else to open/register and electronic money/electronic wallet account to conceal the identity of the Beneficial Owner.

2. Using electronic money/electronic wallet accounts to store funds from misappropriated donations.

3. Using transfer features, including cross-border transactions and/or cash out to transfer funds used to finance terrorist activity.

4. Using the purchase & payment feature to purchase bomb-making components and make bombs, as well as pay for transportation and accommodation expenses.

5. High-frequency transactions of relatively small value using several registered and unregistered accounts (structuring).

C. Money Laundering Risk Assessment Analysis

1. Money Laundering Risk by Region

A risk assessment of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers was performed based on region to ascertain which provinces were most at risk of money laundering. All provinces in Indonesia where non-bank electronic money issuers and non-bank electronic wallet service providers are operating were included as objects of the risk assessment. The sectoral risk assessment by region measured the threats, vulnerabilities and consequences in each respective province based on predetermined risk factors.

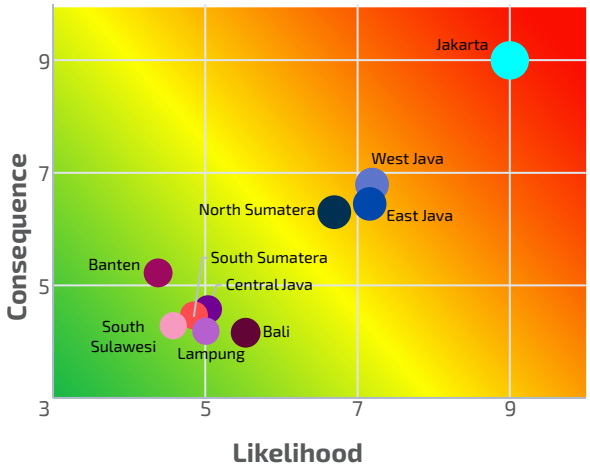
Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability. The main results of the risk analysis by region of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers are presented in Table 4.1.

The results of mapping money laundering risk in non-bank electronic money issuers and non-bank electronic wallet service providers by region is presented in Figure 4.1.

Table 4.1. Risk Analysis of Money Laundering in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Jakarta	9.00	9.00	9.00	9.00	9.00	High
2.	West Java	6.38	7.98	6.75	7.18	6.96	Medium
3.	East Java	6.15	8.17	6.45	7.16	6.80	Medium
4.	North Sumatra	5.92	7.47	6.30	6.69	6.49	Medium
5.	Others	3.58	5.56	3.74	4.57	4.11	Low

Figure 4.1. ML Risk Heatmap by Region in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



Based on the risk heatmap presented in Figure 4.1, the **Special Capital Region of Jakarta** is the only province with a **high** level of money laundering risk in non-bank electronic money issuers and non-bank electronic wallet service providers, followed by **West Java, East Java** and **North Sumatra** as **medium**-risk regions.

Jakarta recorded the highest scores for risk compared to other regions due to the high number of Suspicious Transaction Reports (STR) concerning money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers from 2019-2020.

The provinces of **West Java, East Java** and **North Sumatra** are **medium**-risk regions, primarily due to high vulnerability and consequence scores. The high consequence score was reflected in the high value of money laundering cases that occurred in those provinces, yet still lower than in Jakarta.

Meanwhile, the high vulnerability score was influenced by the level of AML/CFT implementation by service providers in those provinces as well as the perception of law enforcement agencies concerning constraints to the handling of cases in regions where the offences occur. The level of emerging risks in those four provinces is also higher than in other regions given their status as business, economic, financial and government centres.

2. Money Laundering Risk by Corporate Customer Profile

According to money laundering risk analysis based on actors in the National Risk Assessment of Money Laundering 2021, corporate and individual customer profiles were shown to be high risk domestically. Although there are currently no electronic money and electronic wallet features available to corporate customers, a risk assessment of money laundering based on corporate customer profile was also performed to ascertain which business customers potentially posed the most risk of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers.

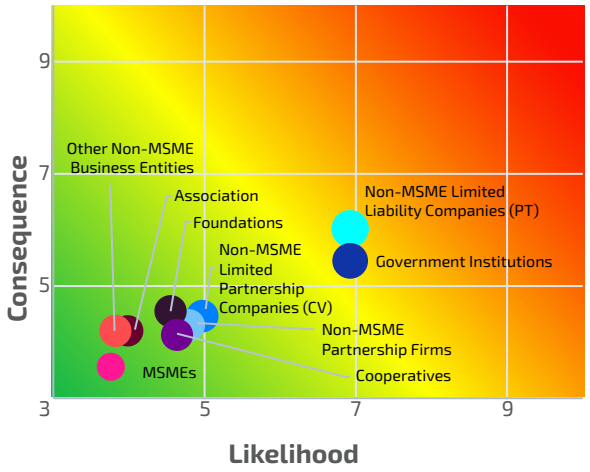
The results of money laundering risk analysis in non-bank money changers based on corporate customer profile in the form of risk are presented in Table 4.2.

Table 4.2. Risk Analysis of Money Laundering in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Corporate Customer Profile

No	Business Entity	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Non-MSME Limited Liability Companies (PT)	6.45	7.36	5.64	6.91	**6.24**	Medium
2.	Government Institutions	5.89	7.25	5.45	6.57	**5.98**	Medium
3.	Others	4.50	4.20	4.16	4.35	**4.25**	Low

The results of mapping money laundering risk in non-bank electronic money issuers and non-bank electronic wallet service providers by corporate customer profile are presented in Figure 4.2

Figure 4.2. ML Risk Heatmap by Corporate Customer Profile in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



According to the risk heatmap presented in Figure 4.2, **Non-MSME Limited Liability Companies (PT)** and **Government Institutions (including state/regional-owned enterprises)** are potentially **medium**-risk business entities concerning money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers. This is because both corporate customer profiles have a significant consequence on the financial system and economy.

3. Money Laundering Risk based on Individual Customer Profile

Money laundering risk was also assessed based on individual customer profile to ascertain which professions were most at risk to committing money laundering via non-bank electronic money issuers and non-bank electronic wallet service providers. The customer profiles used in this assessment refer to the National Risk Assessment of Money Laundering 2021. The risk assessment based on individual customer profile for non-bank electronic money issuers and non-bank electronic wallet service providers had the following limitations, namely the obligation for all non-bank electronic money issuers and non-bank electronic wallet service providers to keep records based on customer profile in accordance with Article 51 of the Bank Indonesia Regulation (PBI) concerning Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT)[44].

According to the risk scores, the results of money laundering risk analysis in non-bank electronic money issuers and non-bank electronic wallet service providers based on individual customer profile are presented in Table 4.3.

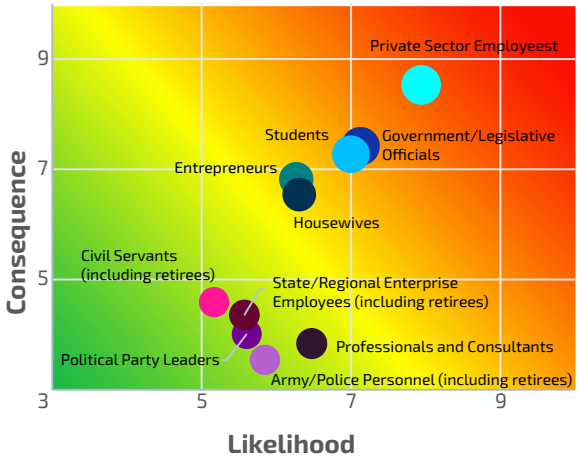
44 Non-bank electronic money issuers and non-bank electronic wallet service providers are required to keep records and data based on customer profile for at least five years after the business relationship with the customer has ended or unusual transactions are identified based on the risk profile of the customer.

Table 4.3. Risk Analysis of Money Laundering in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Individual Customer Profile

No	Risk	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Private Sector Employees	8.84	5.94	8.53	7.39	**7.94**	High
2.	Government/Legislative Officials	5.25	9.00	7.40	7.13	**7.26**	High
3.	Students	7.99	5.62	7.25	7.00	**7.12**	High
4.	Entrepreneurs	6.02	6.50	6.85	6.38	**6.61**	Medium
5.	Housewives	6.42	6.38	6.56	6.40	**6.48**	Medium
6.	Others	4.23	6.17	3.97	5.20	**4.55**	Low

The results of mapping money laundering risk in non-bank electronic money issuers and non-bank electronic wallet service providers by individual customer profile are presented in Figure 4.3

Figure 4.3. ML Risk Heatmap by Individual Customer Profile in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



According to the risk heatmap presented in Figure 4.3, **Private Sector Employees, Students** and **Government/Legislative Officials** are **high** risk for money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers, while **Entrepreneurs** and **Housewives** are **medium**-risk customer profiles. Based on the Sectoral Risk Assessment in 2019, a shift has occurred in terms of risk associated with **Students** given rapid growth of the student customer profile in non-bank electronic money issuers and non-bank electronic wallet service providers.

Private Sector Employees and **Students** are high-risk customer profiles due to the high threat and consequence scores, as reflected by the high frequency and value of Suspicious Transaction Reports (STR) from 2019-2020.

Meanwhile, **Government/Legislative Officials** are a high-risk customer profile due to the high vulnerability and consequence scores. Such conditions are consistent with Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning the Implementation of Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) Non-Bank Payment System Service Providers and Non-Bank Money Changers, as well as the FATF Guidance on Politically Exposed Persons (PEPs), which states that politically exposed persons are highly vulnerable to money laundering crimes. Consequently, prospective customers, customers and beneficial owners categorised as Politically Exposed Persons are treated as high-risk customers.

Entrepreneurs and **Housewives** are medium-risk customer profiles of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers based on a medium consequence score and high threat score given the frequency and value of Suspicious Transaction Reports (STR) from 2019-2020. Meanwhile, the risks associated with Entrepreneurs are influenced by a medium vulnerability score. According to the analysis, Entrepreneurs are vulnerable to illicit activities. Based on the Strategic Analysis report of Housewives conducted by the Financial Monitoring Unit of the Government of Pakistan, housewives pose a money laundering risk using the names of family members to conceal the identity of the beneficial owner using the illicit proceeds of crime as a funding source.

4. Money Laundering Risk based on Products and Services

Money laundering risk was also assessed based on the products and services to ascertain which were most at risk to cases of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers. The products of non-bank electronic money issuers and non-bank electronic wallet service providers are purchase & payment, money transfers for registered users, redeeming points (closed loop), cash out, post-paid or PayLater as well as ATM card data storage. Cash and cashless top up features are also available for electronic money.

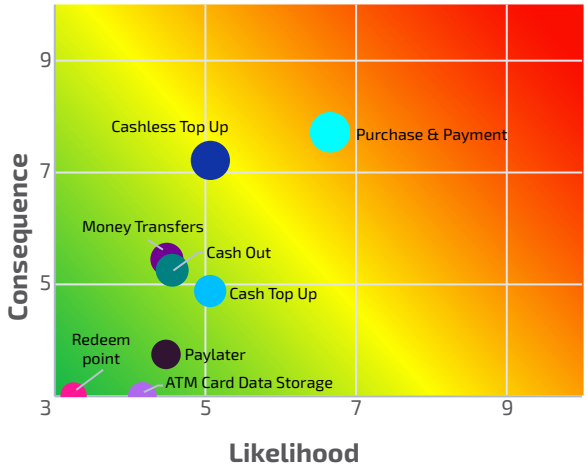
Table 4.4. Risk Analysis of Money Laundering in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Product and Service

No	Product and Service	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Purchase and Payment	8.11	5.20	7.72	6.66	7.17	High
2.	Cashless Top Up	5.02	5.12	7.23	5.07	6.05	Medium
3.	Others	4.35	4.32	4.22	4.34	4.28	Low

The results of money laundering risk analysis in non-bank electronic money issuers and non-bank electronic wallet service providers based on products and services using several risk factors in the form of risk are presented in Table 4.4.

The results of mapping money laundering risk in non-bank electronic money issuers and non-bank electronic wallet service providers by product and service is presented in Figure 4.4.

Figure 4.4. ML Risk Heatmap by Product and Service in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



According to the risk heatmap presented in Figure 4.4, **Purchase & Payment** is a **high**-risk product for money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers, while **Cashless Top Up** is **medium** risk. All other products and services are **low** risk. Based on the Sectoral Risk Assessment in 2019, a shift in risk has occurred to the Purchase & Payment product considering the increases recorded in terms of frequency and value of electronic money as a payment instrument. Furthermore, the Covid-19 pandemic has accelerated the use of digital payments in Indonesia.

Purchase & Payment products recorded high values of threat and consequence, influenced by the high frequency and value of Suspicious Transaction Reports (STR) in 2019-2020. In addition, the rapid emergence of money laundering tYpologies in the form of purchasing online game vouchers and making payments via illegal websites using electronic money also elevated the level of risk associated with **Purchase & Payment** products. Furthermore, **Purchase & Payment** products are vulnerable to Trade-Based Money Laundering where the seller and buyer conspire to create fictitious transactions exploiting purchase & payment features.

Cashless Top Up is a **medium-risk** product for money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers due to the medium threat and high consequence scores, as reflected by the high frequency and value of suspicious transaction reports from 2019-2020. This was influenced by growth in the proportion of transactions initiated via digital services and cashless transactions. Furthermore, the Covid-19 pandemic has triggered a shift in public preferences towards cashless transactions to break the domestic chain of coronavirus transmission.

Meanwhile, the vulnerability score for Purchase & Payment as well as Cashless Top Up products is medium because most non-bank electronic money issuers and non-bank electronic wallet service providers already implement effective anti-money laundering policy, such as by placing limits on transaction value and frequency.

5. Money Laundering Risk based on Delivery Channel

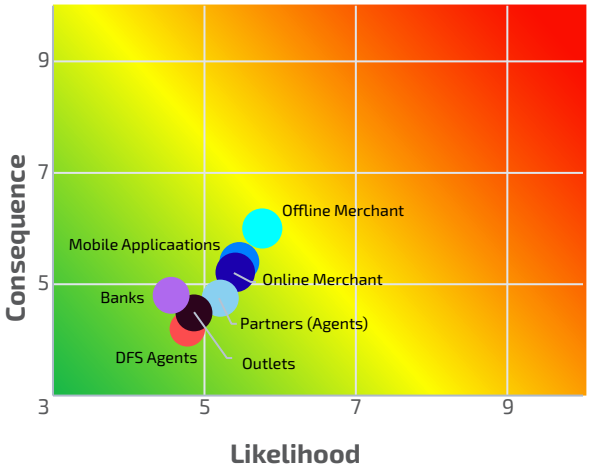
Money laundering risk was also assessed based on the delivery channel to ascertain which were most at risk to cases of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers. The delivery channels of non-bank electronic money issuers and non-bank electronic wallet service providers are the channels by which customers register as users as well as the delivery channels by which customers can utilise the products and services of non-bank electronic money issuers and non-bank electronic wallet service providers, including outlets, mobile applications, DFS agents, offline merchants, online merchants, banks (ATM and/or mobile/SMS/internet banking) as well as agents of non-bank electronic money issuers and non-bank electronic wallet service providers.

Using risk factors in the form of risk, the level of risk for each delivery channel in non-bank electronic money issuers and non-bank electronic wallet service providers was assessed and the results are presented in Table 4.5.

The results of mapping money laundering risk in non-bank electronic money issuers and non-bank electronic wallet service providers by delivery channel is presented in Figure 4.5.

According to the risk heatmap presented in Figure 4.5, **Offline Merchants, Mobile Applications** and **Online Merchants** are **medium-risk** delivery channels for money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers, while all other delivery channels are **low risk**.

Figure 4.5. ML Risk Heatmap by Delivery Channel in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



Offline Merchants recorded the highest risk scores compared to other delivery channels due to a weak customer identification process, coupled with the increasing frequency of payment transactions using electronic money via offline merchants in various regions of Indonesia in line with the rapid development of digital payments in the country.

Mobile Applications, as the medium used to register and transact digitally, received higher risk scores than other delivery channels, including **Online Merchants**. This is due to the non-face-to-face registration and transaction processes, which create risks in terms of using the identity of a third person

Table 4.5. Risk Analysis of Money Laundering in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Offline Merchants	6.00	5.53	6.00	5.76	**5.88**	Medium
2.	Mobile Applications	5.40	5.52	5.40	5.46	**5.43**	Medium
3.	Online Merchants	5.25	5.53	5.20	5.39	**5.29**	Medium
4.	Others	4.81	4.88	4.56	4.85	**4.70**	Low

or false identification documents to conceal the identity of the beneficial owner. Based on FATF Recommendation 8, non-face-to-face transactions have specific risks that require specific rules and procedures to mitigate. In addition, **Online Merchants** are also vulnerable to trade-based money laundering. Notwithstanding, most non-bank electronic money issuers and non-bank electronic wallet service providers implement effective Anti-Money Laundering policies, such as liveness detection for face recognition in the e-KYC process.

D. Terrorist Financing Risk Assessment Analysis

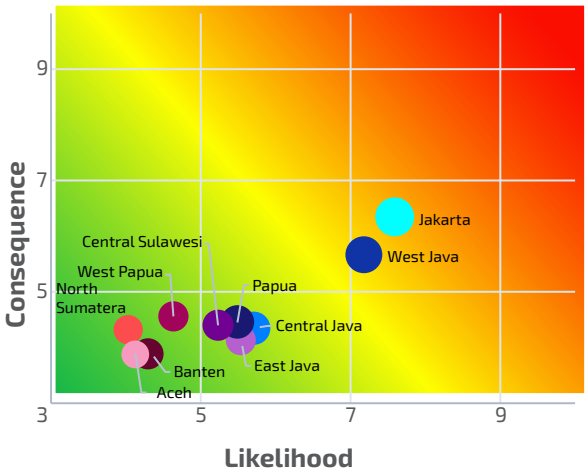
1. Risk Analysis by Region

Terrorist financing risk in non-bank electronic money issuers and non-bank electronic wallet service providers was assessed by region to find out which provinces were most at risk of terrorist financing. The risk analysis by region was performed for all Indonesian provinces where non-bank electronic money issuers and non-bank electronic wallet service providers are located based on the level of risk in each respective province, measured in accordance with the predetermined risk factors.

Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability scores. The salient outcomes of the risk analysis by region of terrorist financing in non-bank Money or Value Transfer Services are recapitulated in Table 4.6.

The results of mapping terrorist financing risk in non-bank electronic money issuers and non-bank electronic wallet service providers by region is presented in Figure 4.6

Figure 4.6. TF Risk Heatmap by Region in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



Based on the risk heatmap presented in Figure 4.6, the **Special Capital Region of Jakarta** and **West Java** are the only provinces with a **medium** level of terrorist financing risk in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers.

Jakarta and **West Java** recorded the highest values of risk compared with other regions. High threat and consequence scores were reflected in the higher number of Suspicious Transaction Reports (STR) with indications of terrorist financing in both provinces.

Meanwhile, the vulnerability score was influenced by AML/CFT implementation by non-bank electronic money issuers and non-

Table 4.6. Risk Analysis of Terrorist Financing in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Province

No	Province	Threat	Vulnerability	Consequence	tLikelihood	Risk Score	Risk Category
1.	Jakarta	8.25	6.93	6.33	7.59	**6.93**	Medium
2.	West Java	7.50	6.86	5.67	7.18	**6.38**	Medium
3.	Others	4.04	4.23	4.16	4.14	**4.15**	Low

bank electronic wallet service providers and the perception of law enforcement agencies concerning constraints to handling terrorism cases in both regions. The emerging risks identified in Jakarta and West Java are also higher than in other provinces as business, economic and financial centres that facilitate the collection, transfer and use of terrorist financing.

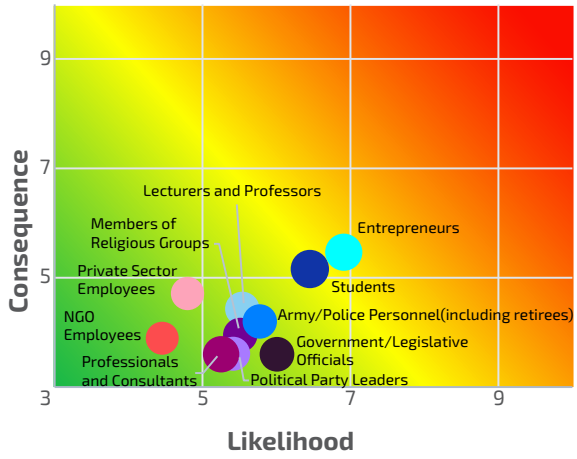
2. Terrorist Financing Risk based on Individual Customer Profile

Terrorist financing risk was also assessed based on individual customer profile to ascertain which professions were most at risk to financing terrorists via non-bank electronic money issuers and non-bank electronic wallet service providers. The risk assessment based on individual customer profile for non-bank electronic money issuers and non-bank electronic wallet service providers had the following limitations, namely the obligation for all non-bank electronic money issuers and non-bank electronic wallet service providers to keep records based on customer profile in accordance with Article 51 of the Bank Indonesia Regulation (PBI) concerning Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT)[45].

According to the risk scores, the results of terrorist financing risk analysis in non-bank electronic money issuers and non-bank electronic wallet service providers based on individual customer profile are presented in Table 4.7.

The results of mapping terrorist financing risk in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by individual customer profile is presented in Figure 4.7

Figure 4.7. TF Risk Heatmap by Individual Customer Profile in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



According to the TF risk heatmap presented in Figure 4.7, **Entrepreneurs** and **Students** are **medium-risk** individual customer profiles for terrorist financing in non-bank electronic money issuers and non-bank electronic wallet service providers, while all other individual customer profiles are **low** risk.

Entrepreneurs and **Students** recorded high scores in terms of threat and medium scores for consequence, as reflected in the high frequency and value of Suspicious Transaction Reports (STR) relating to terrorist financing in 2019-

45 Non-bank electronic money issuers and non-bank electronic wallet service providers are required to keep records and data based on customer profile for at least five years after the business relationship with the customer has ended or unusual transactions are identified based on the risk profile of the customer.

Table 4.7. Risk Analysis of Terrorist Financing in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Individual Customer Profile

No	Profession	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Entrepreneurs	5.65	7.79	5.40	6.72	**6.02**	Medium
2.	Students	5.70	6.70	5.17	6.20	**5.66**	Medium
3.	Others	3.35	5.56	3.17	4.45	**3.74**	Low

2020. The increase of suspicious transaction reports pertaining to **Students** is in line with rapid growth of that customer profile.

Entrepreneurs also received the highest vulnerability score compared with other customer profiles. The National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021 showed that collection activities carried out legally through legitimate business units are one of the most common typologies for collecting terrorist funds. **Entrepreneurs**, therefore, are considered vulnerable to fund collection activities for terrorist financing. The vulnerability of students was influenced by greater internet use amongst students. The vulnerability stems from terrorist groups actively exploiting technological developments to recruit new members through online media.

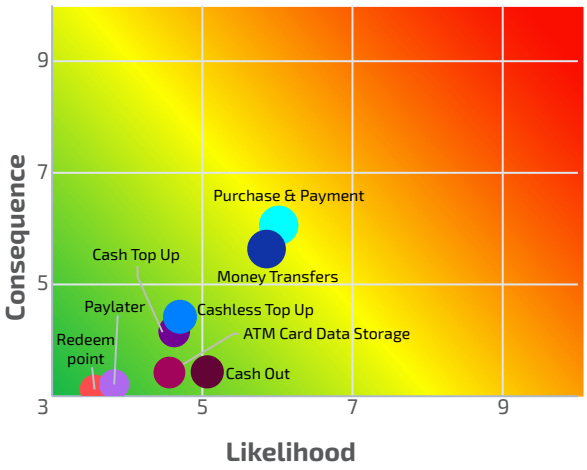
3. Terrorist Financing Risk based on Products and Services

Terrorist financing risk was also assessed based on the products and services to ascertain which were most at risk to cases of money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers. The products of Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers are purchase & payment, money transfers for registered users, redeeming points (closed loop), cash out, post-paid or PayLater, as well as ATM card data storage. Cash and cashless top up features are also available for electronic money.

The results of terrorist financing risk analysis in non-bank electronic money issuers and non-bank electronic wallet service providers based on products and services using several risk factors in the form of risk are presented in Table 4.8.

The results of mapping terrorist financing risk in non-bank electronic money issuers and non-bank electronic wallet service providers by product and service is presented in Figure 4.8.

Figure 4.8. TF Risk Heatmap by Product and Service in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



According to the risk heatmap presented in Figure 4.8, **Purchase & Payment** and **Money Transfers** are considered **medium-risk** products for terrorist financing in non-bank electronic money issuers and non-bank electronic wallet service providers, while all other products and services are **low** risk.

Purchase & Payment and **Money Transfers** received high threat and medium consequence scores, as reflected by the high frequency and

Table 4.8. Risk Analysis of Terrorist Financing in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Product and Service

No	Product and Service	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Purchase and Payment	6.91	5.13	6.05	6.02	**6.03**	Medium
2.	Money Transfers (for registered customers)	7.08	4.63	5.65	5.86	**5.57**	Medium
3.	Others	4.17	4.47	3.28	4.32	**3.76**	Low

value of Suspicious Transaction Reports (STR) from 2019-2020 in line with the increasing frequency and value of transactions via digital services. Furthermore, the Covid-19 pandemic has also accelerated the uptake of digital payments in Indonesia.

Purchase & Payment and **Money Transfers** also represent an emerging risk compared to other products and services. **Purchase & Payment** are vulnerable to exploitation for the purchase of explosives, booking transportation tickets and/or paying for accommodation through e-commerce platforms. Meanwhile, money transfers can be used to transfer and collect funds under the guise of donations.

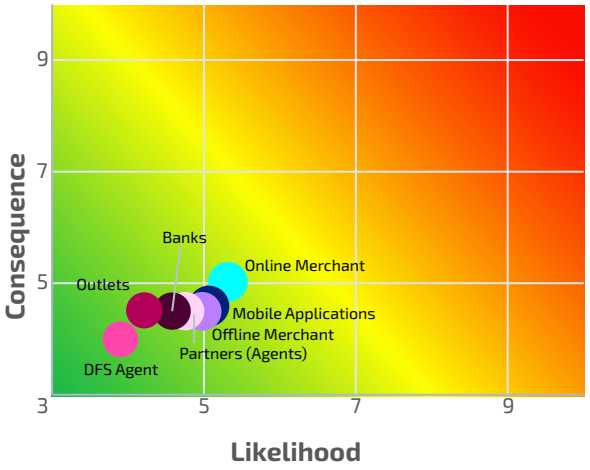
4. Terrorist Financing Risk based on Delivery Channel

Terrorist financing risk was also assessed based on the delivery channel to ascertain which were most at risk to cases of terrorist financing in non-bank electronic money issuers and non-bank electronic wallet service providers. The delivery channels of non-bank electronic money issuers and non-bank electronic wallet service providers are the channels by which customers register as users as well as the delivery channels by which customers can utilise the products and services of non-bank electronic money issuers and non-bank electronic wallet service providers, including outlets, mobile applications, DFS agents, offline merchants, online merchants, banks (ATM and/or mobile/SMS/internet banking) as well as agents of non-bank electronic money issuers and non-bank electronic wallet service providers.

Using risk factors in the form of risk, the level of risk for each delivery channel in non-bank electronic money issuers and non-bank electronic wallet service providers was assessed and the results are presented in Table 4.9.

The results of mapping terrorist financing risk in non-bank electronic money issuers and non-bank electronic wallet service providers by delivery channel is presented in Figure 4.9.

Figure 4.9. TF Risk Heatmap by Delivery Channel in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers



According to the risk heatmap presented in Figure 4.9, **Online Merchants** are a **medium-risk** delivery channel for terrorist financing in non-bank electronic money issuers and non-bank electronic wallet service providers, while all other delivery channels are **low risk**.

Online Merchants recorded the highest vulnerability score compared with other delivery channels due to the proliferation of buying and selling transactions via e-commerce platforms coupled with the volume and value growth of payment transactions using electronic money. Based on the analysis,

Table 4.9. Risk Analysis of Terrorist Financing in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Online Merchants	5.00	5.63	5.00	5.35	**5.16**	Medium
2.	Others	4.38	4.75	4.43	4.57	**4.50**	Low

transactions through **Online Merchants** can be exploited by terrorists to purchase explosives, book transportation tickets and/or pay for accommodation through e-commerce platforms. Notwithstanding, most non-bank electronic money issuers and non-bank electronic wallet service providers already apply effective counter-terrorist financing policies, such as liveness detection for face recognition in the e-KYC process

3

RISK MITIGATION

A. Institutional Aspects of Risk Mitigation

1. Non-bank electronic money issuers and non-bank electronic wallet service providers in Indonesia must be licensed by Bank Indonesia.
2. Non-bank electronic money issuers are not permitted to make changes to the controlling shareholders for five years from the licence date, except under specific conditions approved by Bank Indonesia.
3. Bank Indonesia conducts fit and proper tests of the controlling shareholders, members of the board of directors and members of the board of commissioners of non-bank financial institutions applying for a licence to operate as a non-bank electronic money issuer.
4. At least 15% of the shareholdings must be owned by Indonesian citizens and/or Indonesian business entities, and at least 51% of the shares with voting rights must be owned by Indonesian citizens and/or Indonesian business entities.
5. Bank Indonesia may determine the validity period of a PJP licence as required based on licence category, business activity and/or the source of funding.
6. Bank Indonesia will evaluate the PJP licence every three years or as required.
7. Electronic money issuers wishing to operate as digital financial services (DFS) providers must first obtain approval from Bank Indonesia. Digital financial services are offered by DFS providers through cooperation with DFS agents as individuals/business entities. DFS offered through individual DFS agents can only be provided by DFS providers in the form of a bank.
8. Licensed electronic money issuers wishing to develop new products and/or activities and/or cooperate with a third party must first obtain approval from Bank Indonesia.

B. Operational Aspects of Risk Mitigation

a. Pre-Transaction Mitigation Measures

1. Directors and Board of Commissioners supervise AML/CFT program implementation.
2. Non-bank electronic money issuers and non-bank electronic wallet service providers implement employee screening, customer due diligence and employee capacity building.
3. Non-bank electronic money issuers and non-bank electronic wallet service providers implement robust internal control measures, including regular independent audits, to test AML/CFT implementation compliance and effectiveness.
4. Non-bank electronic money issuers and non-bank electronic wallet service providers identify, assess, control and mitigate risk.
5. Non-bank electronic money issuers and non-bank electronic wallet service providers are required to identify and assess the money laundering and terrorist financing risks as well as control and mitigate the risks prior to developing new products and/or using new technologies.
6. Non-bank electronic money issuers and non-bank electronic wallet service providers are not permitted to receive, use, connect or process electronic money or electronic wallet payment transactions using virtual currencies.

b. Transaction Mitigation Measures

1. Non-bank electronic money issuers and non-bank electronic wallet service providers are required to access databases for customer screening in relation to politically exposed persons (PEP) and the List of Suspected Terrorists and Terrorist Organisations (DTTOT) as well as the List of Proliferation Financing, including international databases.

2. Non-bank electronic money issuers and non-bank electronic wallet service providers apply Regulatory Technology (RegTech) in the implementation of risk-based Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT).

3. Non-bank electronic money issuers and non-bank electronic wallet service providers access the databases of competent authorities, such as the Directorate General of Population and Civil Registration of Indonesia and Legal Entity Administration System, to assist the customer identification and verification process.

4. Non-bank electronic money issuers and non-bank electronic wallet service providers identify and verify prospective customers.

5. Non-bank electronic money issuers and non-bank electronic wallet service providers implement enhanced due diligence for high-risk prospective customers, customers and beneficial owners.

6. Non-bank electronic money issuers and non-bank electronic wallet service providers apply e-KYC principles by requiring customers to register using a registered mobile phone number (in accordance with Communication and Informatics Ministerial Regulation) and send a copy of the national ID card and a photo of the customer holding the national ID card to prevent the use of identification documents that do not match the customer profile.

7. The limit on unregistered electronic money which may be stored in an electronic wallet is Rp2 million and Rp10 million for registered electronic money, with transactions limited to Rp20 million per month based on incoming transactions.

8. Unregistered electronic money cannot be used in funds transfers.

9. Value limits on cash top ups through agents and volume limits on cash and cashless top ups in one day are required.

10. Daily, weekly and/or monthly limits on total transaction value and volume for transfers to bank accounts must be applied.

11. Value limits per transaction and per day for cash out transactions at non-card ATMs must be applied.

c. Post-Transaction Mitigation Measures

1. Non-bank electronic money issuers and non-bank electronic wallet service providers implement identification and verification procedures, data, information and document management as well as reporting to competent authorities.

2. Non-bank electronic money issuers and non-bank electronic wallet service providers identify and report suspicious transactions to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

d. Additional Risk Mitigation Measures Relating to Terrorist Financing

1. Non-bank electronic money issuers and non-bank electronic wallet service providers block or freeze funds belonging to individuals or corporations identified on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).

2. Non-bank electronic money issuers and non-bank electronic wallet service providers conduct rigorous investigations concerning the modus operandi and typologies of terrorist financing cases used by terrorist groups for more effective preventative measures.

3. Non-bank electronic money issuers and non-bank electronic wallet service providers administrate and update the List of Suspected Terrorists and Terrorist Organisations (DTTOT) and relevant UN Security Council Resolutions based on automatic screening to mitigate terrorist financing.

4. Non-bank electronic money issuers and non-bank electronic wallet service providers subscribe to international databases, such as World-Check, in relation to Politically Exposed Persons (PEP) and the List of Suspected Terrorists and Terrorist Organisations (DTTOT) to mitigate terrorist financing.

5. Non-bank electronic money issuers and non-bank electronic wallet service providers implement enhanced due diligence for high-risk prospective customers, customers and beneficial owners to mitigate the exploitation of immediate family members, including wives, children and others, to finance terrorism.

6. In terms of collaborating with third parties, such as agents or partners, non-bank electronic money issuers and non-bank electronic wallet service providers ensure adequate AML/CFT implementation by the third party.

C. Supervision Aspects of Risk Mitigation

1. Bank Indonesia conducts direct and indirect risk-based supervision in relation to AML/CFT implementation by non-bank electronic money issuers and non-bank electronic wallet service providers.

2. Bank Indonesia performs thematic supervision of non-bank electronic money issuers and non-bank electronic wallet service providers.

3. Bank Indonesia may assign other parties for and on behalf of Bank Indonesia to perform inspections of non-bank electronic money issuers and non-bank electronic wallet service providers.

4. For Bank Indonesia supervision, non-bank electronic money issuers and non-bank electronic wallet service providers must identify, manage and update data concerning the Beneficial Owners, while ensuring the availability of data on Beneficial Owners in the interest of Bank Indonesia supervision.

4

CONCLUSIONS

A. Money Laundering Risks

Based on the outcome of statistical data analysis and the risk score of sectoral money laundering in non-bank electronic money issuers and non-bank electronic wallet service providers by **region (province), customer profile, product** and **service** as well as **delivery channel**, the following conclusions were drawn:

1. The **Special Capital Region of Jakarta** is a **high-risk** region for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers, followed by the provinces of **West Java, East Java** and **North Sumatra** as **medium-risk** regions. All other provinces are **low** risk.

2. **Private Sector Employees, Politically Exposed Persons (PEP)** and **Students** are **high-risk** individual customer profiles for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers, followed **Entrepreneurs** and **Housewives** as **medium** risk. All other individual customer profiles are **low** risk.

3. **Non-MSME Limited Liability Companies (PT)** and **Government Institutions (including state/regional-owned enterprises)** are **medium-risk** institutional customer profiles for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other institutional customer profiles are **low** risk.

4. **Purchase** & **Payment** is considered a **high-risk** product for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers, followed by **Cashless Top Up** as **medium** risk. All other products and services of non-bank electronic money issuers and non-bank electronic wallet service providers are **low** risk.

5. **Offline Merchants, Mobile Applications** and **Online Merchants** are **medium-risk** delivery channels for money laundering activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other delivery channels are **low** risk.

Table 4.10. Outcome of Sectoral Risk Assessment of Money Laundering in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers

Risk	Province	Profession	Business Entity	Product/Service	*Delivery Channel*
High	Jakarta	Private Sector Employees , PEP, Students	-	Purchase and Payment	-
Medium	West Java, East Java, North Sumatra	Entrepreneurs, Housewives	Non-MSME Limited Liability Companies (PT), Government Institutions	Cashless Top Up	Offline Merchant, Mobile Application, Online Merchant
Low	Others	Others	Others	Others	Others

B. Terrorist Financing Risk

Based on the outcome of statistical data analysis and emerging risks of terrorist financing in non-bank electronic money issuers and non-bank electronic wallet service providers by **region (province), customer profile, product** and **service** as well as **delivery channel**, the following conclusions were drawn:

1. The **Special Capital Region of Jakarta** and **West Java** are **medium-risk** regions for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other provinces are **low** risk.
2. **Entrepreneurs** and **Students** are **medium-risk** individual customer profiles for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other individual customer profiles are **low** risk.
3. **Money Transfers** and **Purchase & Payment** are **medium-risk** products for terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other products and services are **low** risk.
4. **Online Merchants** are a **medium-risk** delivery channel concerning terrorist financing activity in non-bank electronic money issuers and non-bank electronic wallet service providers. All other delivery channels are **low** risk.

Table 4.11. Outcome of Sectoral Risk Assessment of Terrorist Financing in Non-Bank Electronic Money Issuers and Non-Bank Electronic Wallet Service Providers

Risk	Province	Profession	Product/Service	Delivery Channel
High	-	-	-	-
Medium	Jakarta, West Java	Entrepreneurs, Students	Money Transfer, Purchase and Payment	Online Merchants
Low	Others	Others	Others	Others


CREDIT
CARD
Rp
Rp

PART II

NON-BANK CARD-BASED PAYMENT INSTRUMENT (CBPI)

EXECUTIVE SUMMARY

In 2021, the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), in conjunction with relevant government ministries/ agencies, identified, analysed and evaluated the latest money laundering, terrorist financing and proliferation financing risks holistically through the national risk assessment program, namely the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021. As a follow-up action to mitigate the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in Non-Bank Card-Based Payment Instrument (CBPI), a sectoral risk assessment (SRA) of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction was performed covering non-bank card-based payment instrument issuers with the following objectives:

1. Identifying and analysing the threats, vulnerabilities and consequences of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the non-bank CBPI sector.

2. Identifying, analysing and evaluating various risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction based on mapping the **customer profiles (individual and corporate), regions (provinces), products and services** as well as **delivery channels** in the non-bank CBPI sector.

3. Identifying and analysing the emerging threats of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the non-bank CBPI sector.

4. Formulating strategic risk mitigation measures against money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the non-bank CBPI sector.

The SRA of money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction in the non-bank CBPI sector mapped four key risks based on customer profile, region, product and service as well as delivery channel and formulated risk factors covering the threats, vulnerabilities and consequences. The analysis methodology referred to the risk assessment method issued by the Financial Action Task Force (FATF). According to the latest assessment, the level of money laundering risk in the non-bank CBPI sector is as follows:

1. The **Special Capital Region of Jakarta** is a **high-risk** region concerning money laundering activity in the non-bank CBPI sector, followed by the provinces of **West Java** and **East Java** as **medium-risk** regions. All other provinces are **low** risk.

2. **Government Institutions** and **Non-MSME Limited Liability Companies (PT)** are **medium-risk** institutional customer profiles for money laundering activity in the non-bank CBPI sector. All other institutional customer profiles are **low** risk.

3. **Politically Exposed Persons (PEP)** are a **high-risk** individual customer profile for money laundering activity in the non-bank CBPI sector, followed **Entrepreneurs** as **medium** risk. All other individual customer profiles are **low** risk.

4. **Purchase & Payment** is a **medium-risk** product for money laundering activity in the non-bank CBPI sector. All other products and services are **low** risk.

5. **Online Merchants** and **ATMs** are **medium-risk** delivery channels for money laundering activity in the non-bank CBPI sector. All other delivery channels are **low** risk.

Based on the latest assessment, the level of terrorist financing risk in non-bank electronic money issuers and non-bank electronic wallet service providers is as follows:

1. The **Special Capital Region of Jakarta** and **East Java** are **medium-risk** regions for terrorist financing activity in the non-bank CBPI sector. All other provinces are **low** risk.

2. **Entrepreneurs** and **Private Sector Employees** are **medium-risk** individual customer profiles for terrorist financing activity in the non-bank CBPI sector. All other individual customer profiles are **low** risk.

3. **Purchase & Payment** is a **medium-risk** product for terrorist financing activity in the non-bank CBPI sector. All other products and services are **low** risk.

4. **Online Merchants** are a **medium-risk** delivery channel for terrorist financing activity in the non-bank CBPI sector. All other delivery channels are **low** risk.

Bank Indonesia has issued regulations and guidelines as well as performed direct and indirect supervision to mitigate the risks associated with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the non-bank CBPI sector. Furthermore, Bank Indonesia actively cooperates domestically and internationally. Meanwhile, Bank Indonesia has also organised socialisation and education activities targeting non-bank card-based payment instrument issuers and members of the public to increase awareness of the risks and support efforts to prevent and eradicate money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction.

1

LITERATURE REVIEW OF NON-BANK CARD-BASED PAYMENT INSTRUMENT (CBPIs)

A. Legal Basis

Bank Indonesia is a supervisory and regulatory body (LPP) for non-bank card-based payment instrument issuers in accordance with Act No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (ML Act). In terms of AML/CFT policies and supervision, Bank Indonesia's authority over the non-bank CBPI sector extends to non-bank card-based payment instrument issuers providing card-based payment instrument services.

Regulations concerning non-bank card-based payment instrument issuers are contained in Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012, as an amendment to Bank Indonesia Regulation (PBI) No. 11/11/PBI/2009, concerning Implementation of Card-Based Payment Instrument Activities, dated 6th January 2012 and Bank Indonesia Circular Letter No. 18/33/DKSP, dated 2nd December 2016, as the fourth amendment to Bank Indonesia Circular Letter No. 11/10/DASP, dated 13th April 2009 concerning Card-Based Payment Instruments. The salient provisions of the Bank Indonesia regulations concerning the implementation of card-based payment instrument activities are as follows:

1. Maximum credit card interest rates, as determined by Bank Indonesia and stipulated in a Bank Indonesia Circular Letter.
2. Minimum cardholder requirements, including age, income and credit ceiling, as well as the maximum number of credit card facilities that an issuer may provide, as stipulated in the corresponding Bank Indonesia Circular Letter.
3. Consumer protection and prudential principles, such as standardised credit card interest rate calculations, fees and fines and information disclosure to cardholders.
4. Cooperation with third parties referring to the Bank Indonesia regulation on outsourcing, particularly in relation to debt collection.
5. Security obligations in the form of mandatory transaction alerts to cardholders.
6. Obligations to provide interconnected and interoperable systems.
7. Bank Indonesia's authority in terms of licensing and sanctioning non-bank card-based payment instrument issuers.

Since July 2021, however, regulations concerning the payment system have been in accordance with Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System (PBI PS) as well as Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning Payment Service Providers (PJP) and Bank Indonesia Regulation (PBI) No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PIP), covering the following:

1. Scope of activities for non-bank payment service providers, payment system infrastructure providers and supporting providers, as well as PJP licensing and PIP determination.
2. Ownership and control.

3. PJP and PIP obligations, including governance, risk management, prudential principles, information systems security standards, interconnectivity and interoperability, infrastructure and regulatory compliance, including AML/CFT.

4. Development of activities, products and/or cooperation based on risk.

5. Corporate actions in the form of mergers, consolidation, separation and/or acquisitions.

6. Source of funds and access to funding sources.

7. Restrictions on PJP from owning and/or managing value equivalent to money or foreign currency that can be used widely for payment purposes, and the absolute prohibition of receiving, using, connecting and/or processing transactions using virtual currency.

Based on the latest payment system regulations, non-bank card-based payment instrument issuers can implement account information services, payment initiation and/or acquiring services as well as PIP activities. In addition, the Bank Indonesia regulation on PJP also regulates payment instrument using cards or card-less (virtual) payment instruments to initiate payment transactions and/or provide access to funding sources for payment. Provisions in the Bank Indonesia regulation on PJP relating to access to funding sources in the form of card-based payment instruments, specifically PJP as credit card issuers are as follows:

1. Obligations to implement credit risk management based on the minimum age and income of cardholders, the credit ceiling based on risk analysis, restrictions on PJP accounts issuance services, as well as minimum credit card payments by cardholders. PJP offering account issuance services are also required to update cardholder data.

2. Obligations to improve security standards for specific transactions by providing transaction alerts to cardholders via previously agreed channels and/or other security standards.

3. Obligations to provide written information covering the procedures, consequences/ risks of use, cardholder rights and obligations, complaint procedures, how interest rates are calculated, credit card fees and fines, procedures for closing credit card facilities as well as periodic statements of credit card activity based on a cardholder request and/or approval.

4. Obligations to submit billing information, offer grace periods and restrictions on fines for cardholders making payments during a grace period.

5. Obligations to formulate and implement credit policies.

6. Compliance obligations to debt collection ethics and guidelines.

B. Characteristics of Non-Bank Card-Based Payment Instrument in Indonesia

Card-based payment instruments include credit cards, automated teller machine (ATM) cards and/or debit cards.[45]

In accordance with Article 1 of the Bank Indonesia Regulation (PBI) on Card-Based Payment Instruments, a credit card is a card-based payment instrument that may be used for payment of liabilities arising from an economic activity, including purchases and/or cash advances, in which the payment obligation of the cardholder must be first fulfilled by an acquirer or issuer, with the cardholder required subsequently to make payment at the agreed time, whether in a lump sum (charge card) or in instalments.[46]

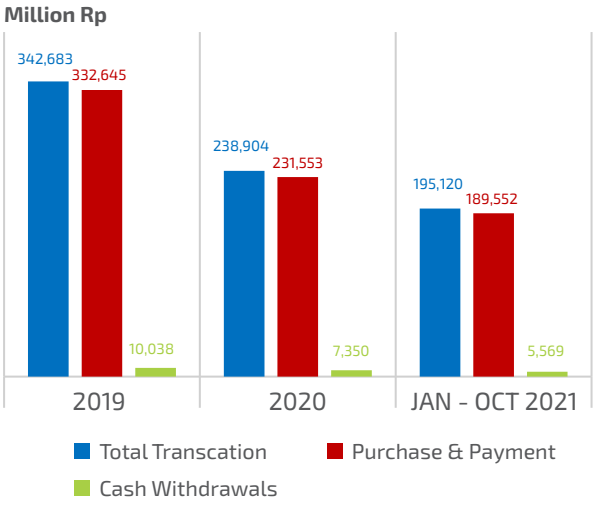
An ATM card is a card-based payment instrument that may be used for cash withdrawals and/or funds transfers in which the obligations of the cardholder must be fulfilled immediately by directly debiting the deposit account of the cardholder with a bank or non-bank financial institution authorised to collect funds based on prevailing laws and regulations.[47]

A debit card is a card-based payment instrument that may be used for payment of obligations arising from an economic activity, including purchases, in which the obligations of the cardholder must be fulfilled immediately by directly debiting the deposit account of the cardholder with a bank or non-bank financial institution authorised to collect funds based on prevailing laws and regulations.[48]

The delivery channels of card-based payment instruments are classified into two categories, namely for the cardholder registration process and for the cardholder to use the products and services. Cardholder registration is possible via an outlet or mobile application, while the products and services can be used via ATM machines (for cash withdrawals), offline merchants, online merchants as well as purchase & payment partners.

As of December 2021, a total of four non-bank financial institutions located in Jakarta were licensed as non-bank card-based payment instrument issuers. Nationally, credit card transactions have experienced a significant 30.3% (yoy) decline due to the impact of the Covid-19 pandemic. As of October 2021, purchase & payment transactions dominated 97% of the total. Spatially, 90% of national credit card transactions occur in just seven provinces, namely the Special Capital Region of Jakarta, East Java, West Java, Banten, North Sumatra, Central Java and Bali. Meanwhile, online transactions accounted for 25% of total purchase & payment transactions as of October 2021, up 19% by 2020.

Graph 5.1. National Card-Based Payment Instrument Transactions



Source: Bank Indonesia

45 Article 1, Paragraph 3 of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Implementation of Card-Based Payment Instrument Activities.

46 Article 1, Paragraph 4 of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Implementation of Card-Based Payment Instrument Activities.

47 Article 1, Paragraph 5 of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Implementation of Card-Based Payment Instrument Activities.

48 Article 1, Paragraph 6 of Bank Indonesia Regulation (PBI) No. 14/2/PBI/2012 concerning Implementation of Card-Based Payment Instrument Activities.

2

KEY RISKS IN NON-BANK CARD-BASED PAYMENT INSTRUMENT

A. Money Laundering Risk Landscape

The typologies of money laundering have evolved in Indonesia to become more complex and varied over time by exploiting financial system institutions. Based on the National Risk Assessment (NRA) of Money Laundering, most money laundering cases in Indonesia stem from the predicate offences of narcotics and corruption. In terms of individual customer profile, most perpetrators of money laundering crimes are Government/ Legislative Officials as well as Employees of State/Regional-Owned Enterprises (including retirees), while Limited Liability Companies (PT) dominate the corporate customer profile side. The Special Capital Region of Jakarta is considered a high-risk province for money laundering cases, with the typologies dominated by the use of false identification documents, nominees, trusts, family members or third parties, property/real estate (including estate agents), smurfing[49], structuring[50], using professional services, using new payment systems/methods, using legal persons and exploiting unregulated sectors.

Card-based payment instruments are one type of payment instrument used as a vehicle to launder money. In accordance with the money laundering typologies released by the Asia-Pacific group (APG) on Money Laundering, credit cards are typically used to access funds in other jurisdictions. The beneficial owner of the credit card is usually difficult to identify, making it easier for exploitation to launder money. This was confirmed in the FATF Guidance for a Risk-Based Approach to New Payment Products and Services published in 2013, stating that difficulties in identifying customers created money laundering risk in card-based payment instruments. The compact size enables card-based payment instruments to be smuggled abroad and misused in other jurisdictions, unlike cash that requires the use of international couriers. Mitigation measures are necessary, therefore, in terms of enforcing credit ceilings and cash withdrawal limits. In addition, the involvement of numerous parties in payments transaction processing, including the principal, acquirer, switching provider and clearing provider, along with final settlement, increases the potential money laundering risks, particularly if those parties are located in different jurisdictions. There are potential difficulties in identifying customer information and transactions, particularly if the party responsible for AML/CFT implementation has not been determined specifically. Furthermore, the investigation process will encounter more constraints. Despite the high risks posed by misuse as a tool to facilitate money laundering, no significant cases of money laundering through non-bank card-based payment instrument issuers have been identified in Indonesia.

In more detail, the salient money laundering risk factors using Non-Bank Card-Based Payment Instrument Issuers are as follows:

1. The compact size enables card-based payment instruments to be smuggled abroad and misused in other jurisdictions.
2. Using encrypted internet protocols, access to identities and international banking. This technique exploits the internet to hack data/ information or defraud victims using false e-mail addresses or websites.
3. Using credit card facilities in the name of another cardholder to conceal the identity of the beneficial owner.

49 Smurfing is a money-laundering technique involving the use of several different accounts on behalf of one customer.

50 Structuring is a money-laundering technique using relatively small, yet high-frequency, transactions in the financial sector.

4. Paying bills on the due date by a third party to conceal the identity of the beneficial owner.

5. Initiating Purchase & Payment as well as Cash Out transactions using the illicit proceeds of crime.

6. Structuring techniques using relatively small, yet high-frequency, transactions.

B. Terrorist Financing Risk Landscape

In the context of terrorist financing and financing of proliferation of weapons of mass destruction in Indonesia, the typologies are becoming more complex and varied, exploiting financial institutions and non-financial institutions. Based on the National Risk Association (NRA) of Terrorist Financing, funds used to finance domestic terrorist activities procured from within the country or abroad as well as funds derived from within Indonesia for foreign terrorist activity are considered high threats. In terms of the typologies, fundraising by terrorist financiers and funds embezzled from donations through community organisations are considered high risk for terrorist activity. In terms of transferring funds, most use financial service providers, specifically banks, money transfer service providers and money changers. Terrorist funds are also considered high risk of being used to purchase arms and explosives, training in the manufacture of arms and explosives as well as travel expenses to and from domestic terrorist operations. Based on individual customer profile, those most at risk of funding terrorists include entrepreneurs, while institutional customers include limited liability companies (PT), foundations, associations and limited partnership companies (CV). Meanwhile, the highest risk provinces were Jakarta, East Java, West Java and Central Java.

Furthermore, the results of mapping foreign inward risk or foreign predicate crime (FPC) based on the NRA showed that the high-risk sources of terrorist financing into Indonesia are the United States, Malaysia, the Philippines and Australia. Meanwhile, mapping the foreign outward risk or laundering offshore (LO) showed that the high-risk destinations for LO include Malaysia, the Philippines and Australia. In addition, there are several emerging threats concerning terrorist financing that must be mitigated moving forward as follows:

1. Terrorist financing by corporate (institutional) sponsors.

2. Narco-terrorism.

3. Use of virtual currency for terrorist financing.

4. Use of online/peer-to-peer lending for terrorist financing.

5. Activities of armed criminal groups in the country.

Non-bank card-based payment instrument issuers could potentially be used as a vehicle for terrorist financing and financing of proliferation of weapons of mass destruction. In accordance with the money laundering typologies identified by the Asia-Pacific group (APG) on Money Laundering, credit cards are typically used to access funds in other jurisdictions. Furthermore, the beneficial owner of the credit card is usually difficult to identify, making it easier for exploitation to finance terrorists. Notwithstanding, no significant terrorist financing cases have been discovered in Indonesia exploiting the non-bank CBPI sector.

In more detail, the salient terrorist financing risk factors using Non-Bank Card-Based Payment Instrument Issuers are as follows:

1. The compact size enables card-based payment instruments to be smuggled abroad and misused in other jurisdictions.

2. Using encrypted internet protocols, access to identities and international banking. This technique exploits the internet to hack data/information or defraud victims using false e-mail addresses or websites.

3. 3Using credit card facilities in the name of another cardholder to conceal the identity of the beneficial owner.

4. Paying bills on the due date by a third party to conceal the identity of the beneficial owner.

5. Initiating Purchase & Payment as well as Cash Out transactions using the illicit proceeds of crime.

6. Structuring techniques using relatively small, yet high-frequency, transactions.

7. Collecting and/or raising funds for terrorist acts using card-based payment instruments.

Utilising funds from credit card facilities for terrorist activity, such as purchasing arms and explosives as well as travel expenses to and from acts of terrorism.

C. Money Laundering Risk Assessment Analysis

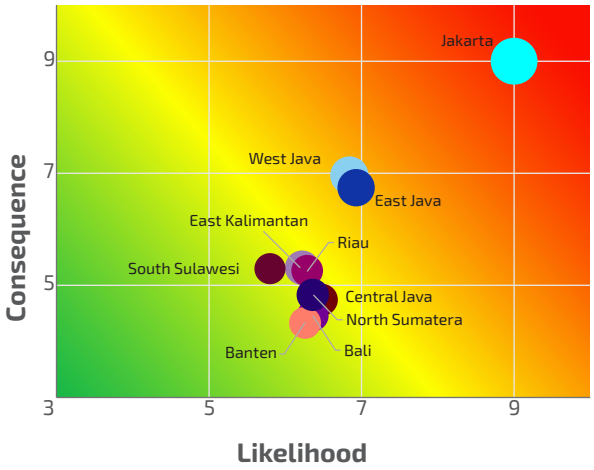
1. Money Laundering Risk by Region

A risk assessment of money laundering in the non-bank CBPI sector was performed based on region to ascertain which provinces posed the highest risk of money laundering cases. The risk assessment by region measured the threats, vulnerabilities and consequences in each respective province based on predetermined risk factors.

Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability. The salient outcomes of the risk analysis by region of money laundering in non-bank CBPI sector are recapitulated in Table 5.1.

The results of mapping money laundering risk in the non-bank CBPI sector by region are presented in Figure 5.1.

Figure 5.1. ML Risk Heatmap by Region in Non-Bank CBPI Sector



Based on the ML risk heatmap presented in Figure 5.1, the **Special Capital Region of Jakarta** is the province with a **high** level of money laundering risk in the non-bank CBPI sector, followed by **West Java** and **East Java** as **medium-risk** regions. All other regions are **low** risk.

The **Special Capital Region of Jakarta** scored the highest risk scores. The results of risk assessments conducted by law enforcement agencies and supervisors confirmed that Jakarta was a high-risk region in terms of money laundering through non-bank card-based payment instrument issuers due to the high number of non-bank card-based payment instrument transactions in Jakarta given the concentration of corporate head offices, thus increasing the potential risk of using card-

Table 5.1. Risk Analysis of Money Laundering in Non-Bank CBPI Sector by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Jakarta	9.00	9.00	9.00	9.00	**9.00**	High
2.	West Java	8.01	6.98	6.91	6.84	**6.91**	Medium
3.	East Java	7.98	6.17	6.65	6.93	**6.80**	Medium
4.	Others	4.57	5.89	4.35	5.06	**4.01**	Low

based payment instruments as a vehicle for money laundering.

The provinces of **West Java** and **East Java** are medium-risk regions for money laundering in the non-bank CBPI sector in line with the perception of law enforcement agencies and supervisors due to large local economies, which increases the potential risk of the non-bank CBPI sector being exploited for money laundering purposes.

National credit card data as of October 2021 showed that 80% of credit card instruments are distributed in just six provinces, namely Jakarta (32%), West Java (17%), East Java (12%), Banten (8%), North Sumatra (7%) and Central Java (5%). On the other hand, transaction value is dominated by the provinces of Jakarta (53%), East Java (10%), West Java (10%), Banten (7%) and North Sumatra (4%).

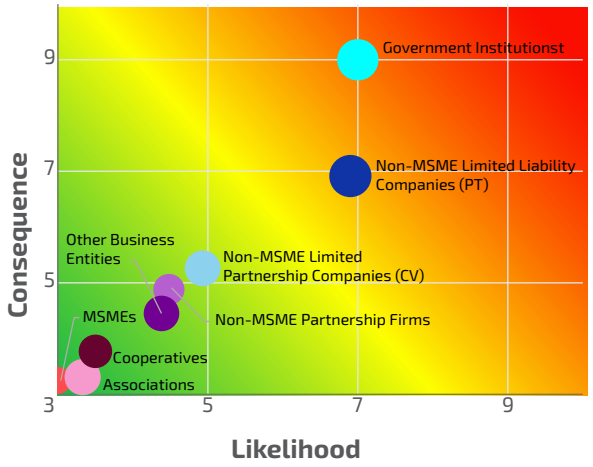
2. Money Laundering Risk

According to money laundering risk analysis based on actors in the National Risk Assessment of Money Laundering 2021, corporate and individual customer profiles were shown to be high risk domestically. Therefore, a risk analysis of money laundering based on business entity was necessary to understand which types of corporate customer profile were most at risk of money laundering in the non-bank CBPI sector.

The results of money laundering risk analysis in the non-bank CBPI sector based on corporate customer profile are presented in Table 5.2.

The results of mapping money laundering risk in the non-bank CBPI sector by corporate customer profile are presented in Figure 5.2.

Figure 5.2. ML Risk Heatmap by Corporate Customer Profile in Non-Bank CBPI Sector



According to the risk heatmap presented in Figure 5.2, **Government Institutions** and **Non-MSME Limited Liability Companies (PT)** are **medium-risk** corporate customer profiles for money laundering in the non-bank CBPI sector. All other business entities are **low** risk. The results are based on analysis performed by law enforcement agencies, reporting parties and supervisors.

Table 5.2. Risk Analysis of Money Laundering in Non-Bank CBPI Sector by Corporate Customer Profile

No	Business Entity	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Government Institutions	6.96	7.00	9.00	7.00	**7.00**	Medium
2.	Non-MSME Limited Liability Companies (PT)	9.00	6.95	6.91	6.90	**6.93**	Medium
3.	Others	6.00	4.87	3.97	3.84	**4.18**	Low

Government Institutions, in this case state/regional-owned enterprises, received the highest potential vulnerability and consequent scores concerning money laundering based on an assessment by law enforcement agencies. Meanwhile, an assessment by reporting parties also showed that **Government Institutions** are a medium-risk corporate customer profile for money laundering in the non-bank CBPI sector.

Non-MSME Limited Liability Companies (PT) received higher threats and consequence scores. An assessment by reporting parties showed that **Non-MSME Limited Liability Companies (PT)** were the dominant corporate customers of non-bank card-based payment instrument issuers, thereby increasing the potential risk of money laundering. This was confirmed by the findings of the National Risk Assessment of Money Laundering in 2021, showing that from 2016-2021 there were several money laundering cases involving corporate customers, specifically **Non-MSME Limited Liability Companies (PT)**.

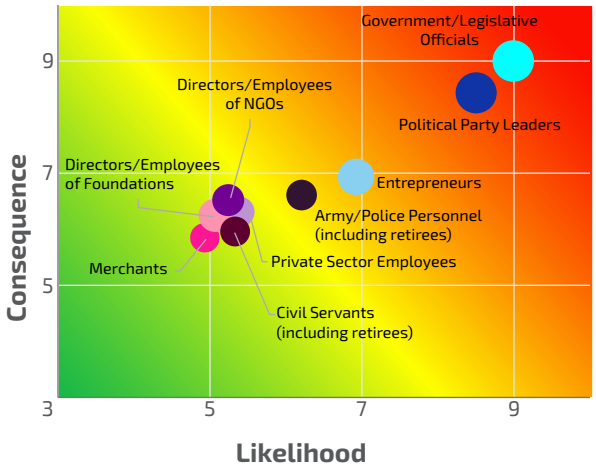
3. Money Laundering Risk based on Individual Customer Profile

Money laundering risk was also assessed based on individual customer profile to ascertain which professions were most at risk to committing money laundering in the non-bank CBPI sector.

The results of money laundering risk analysis in the non-bank CBPI sector based on individual customer profile are presented in Table 5.3.

The results of mapping money laundering risk in the non-bank CBPI sector by individual customer profile is presented in Figure 5.3.

Figure 5.3. ML Risk Heatmap by Individual Customer Profile in Non-Bank CBPI Sector



According to the ML risk heatmap presented in Figure 5.3, **Government/Legislative Officials** and **Political Party Leaders** are **high-risk** customer profiles for money laundering in the non-bank CBPI sector, while **Entrepreneurs** are considered **medium-risk** customer profiles. All other customer profiles are **low** risk.

According to Article 34 of Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) for Non-Bank Payment System Service Providers and Non-Bank Money Changers, and referring to the FATF Guidance for Politically Exposed

Table 5.3. Risk Analysis of Money Laundering in Non-Bank CBPI Sector by Individual Customer Profile

No	Profession	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Government/Legislative Officials	9.00	9.00	9.00	9.00	**9.00**	High
2.	Political Party Leaders	8.52	8.49	8.43	8.50	**8.69**	High
3.	Entrepreneurs	8.67	7.00	6.94	6.91	**6.99**	Medium
4.	Others	5.77	5.00	4.81	5.48	**4.66**	Low

Persons (PEP), customer profiles included in the category of Politically Exposed Persons are particularly vulnerable to money laundering. Therefore, prospective customers, customers and beneficial owners categorised as PEP are considered high risk.

As reported in the National Risk Assessment of Money Laundering 2021, customer profiles categorised as Domestic PEP include **Government/Legislative Officials, State/ Regional Enterprise Employees (including retirees), Civil Servants (including retirees), Army/Police Personnel (including retirees),** Lecturers and Professors serving as University Rectors, as well as **Political Party Leaders**. In addition, considering that customers of non-bank card-based payment instrument issuers are also domiciled abroad, Foreign PEPs are also an area of concern, including **Heads of State** or **Heads of Government, Senior Politicians, Senior Government Officials, Military Officers, Law enforcement agencies, Senior Management of State-Owned Enterprises** as well as **Senior Political Party Members**.

Entrepreneurs received a higher threat score based on an assessment by law enforcement agencies, which was confirmed by the findings of the National Risk Assessment of Money Laundering in 2021, revealing that **Entrepreneurs** represent a high risk in terms of money laundering domestically and internationally as well as laundering money from abroad.

4. Money Laundering Risk based on Products and Services

Money laundering risk was also assessed based on the products and services of non-bank card-based payment instrument issuers to ascertain which were most at risk to cases of money laundering in the non-bank CBPI sector. The risk analysis of products and services in the non-bank CBPI sector had the following limitations:

1. In accordance with the authority of Bank Indonesia, AML/CFT policy and supervision only extends to card-based payment instruments issued by non-bank issuers.

2. As the object of this assessment, credit cards were the only product assessed because non-bank card-based payment instrument issuers are not permitted to issue ATM cards or debit cards in Indonesia.

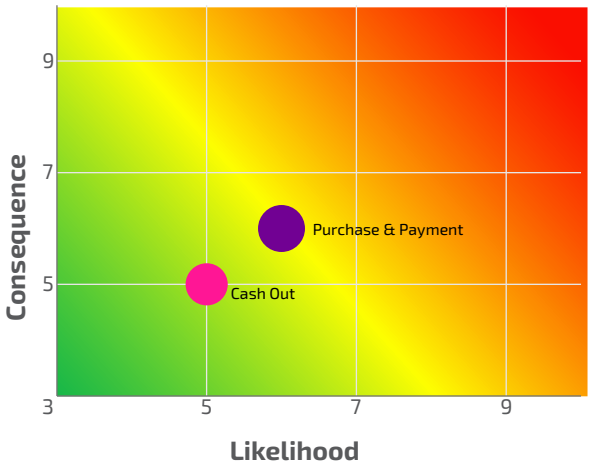
The results of money laundering risk analysis in the non-bank CBPI sector based on products and services using several risk factors in the form of risk are presented in Table 5.4.

The results of mapping money laundering risk in the non-bank CBPI sector by product and service is presented in Figure 5.4.

Table 5.4. Risk Analysis of Money Laundering in Non-Bank CBPI Sector by Product and Service

No	Product and Service	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Purchase and Payment	6.00	6.73	6.00	6.00	**6.00**	Medium
2.	Cash Out	5.00	5.00	5.00	5.00	**5.00**	Low

Figure 5.4. ML Risk Heatmap by Product and Service in Non-Bank CBPI Sector



According to the ML risk heatmap presented in Figure 5.4, **Purchase & Payment** is a **medium-risk** product for money laundering in the non-bank CBPI sector, while **Cash Out** is **low** risk.

Purchase & Payment products recorded medium risk scores based on risk analysis performed by law enforcement agencies and reporting parties. **Purchase & Payment** is a CBPI product that is quick and convenient to use and the beneficial owner is difficult to identify. Notwithstanding, **Purchase & Payment** does not allow the continuous flow of funds and is not as difficult to trace as the **Cash Out** product. Furthermore, a shift has occurred from cash to cashless transactions in response to the Covid-19 pandemic, thereby increasing the potential risks associated with **Purchase & Payment** products.

In addition, the dominance of **Purchase & Payment** in national credit card transactions raises the potential risk of this product being used as a mode for money laundering. National credit card data showed that **Purchase & Payment** transactions dominate 97% of the total, of which 25% are performed online. The share of online transactions increased 19% in 2021 on the previous year in response to 26.6% (yoy) growth of online transactions as of October 2021.

Despite a low-risk classification, **Cash Out** is vulnerable to exploitation as a channel of money laundering considering how convenient and universally available such transactions are, thus hampering the investigation process. Several cases show that **Cash Out** has been used by criminals to conceal funding flows because cash transactions are difficult to trace and track.

5. Money Laundering Risk based on Delivery Channel

Money laundering risk was also assessed based on the delivery channel to ascertain which delivery channels were most at risk to cases of money laundering in the non-bank CBPI sector. The delivery channels of non-bank card-based payment instrument issuers are grouped into two main categories, namely delivery channels for the customer registration process and delivery channels for the customers to use the products and services. Customer registration is facilitated by outlets and mobile applications, while the delivery channels for customers to use the products and services include ATMs (for cash withdrawals), offline merchants, online merchants as well as purchase & payment agents.

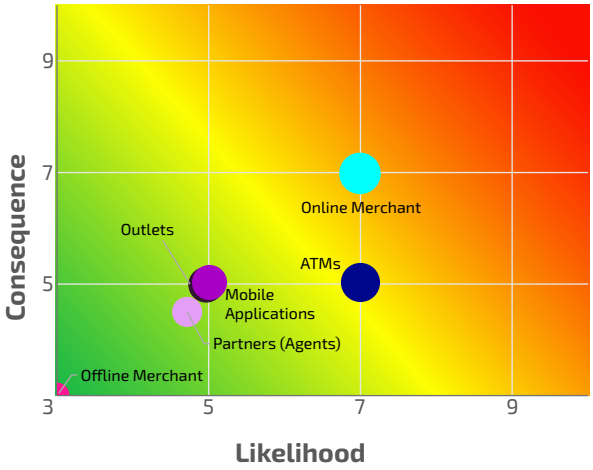
Using risk factors in the form of risk, the level of money laundering risk for each delivery channel in the non-bank CBPI sector was assessed and the results are presented in Table 5.5.

Table 5.5. Risk Analysis of Money Laundering in Non-Bank CBPI Sector by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Online Merchants	5.00	7.55	7.00	7.00	**7.00**	Medium
2.	ATMs	5.00	7.50	5.00	7.00	**7.00**	Medium
3.	Other Delivery Channels	4.25	4.63	4.37	5.79	**5.00**	Low

The results of mapping money laundering risk in the non-bank CBPI sector by delivery channel is presented in Figure 5.5.

Figure 5.5. Risk Heatmap by Delivery Channel in Non-Bank CBPI Sector



According to the ML risk heatmap presented in Figure 5.5, **Online Merchants** are a **high-risk** delivery channel for money laundering in the non-bank CBPI sector, while ATMs are a medium-risk delivery channel. All other delivery channels are **low** risk.

Online Merchants recorded medium threat and consequence scores along with a high vulnerability score based on risk assessments performed by law enforcement agencies and parties. Furthermore, a shift has occurred from cash to cashless transactions in response to the Covid-19 pandemic, thereby increasing the potential risks associated with **Online Merchants** as a delivery channel.

ATMs are a medium-risk delivery channel according to risk assessments by law enforcement agencies and reporting parties. Cash withdrawals via ATM machines are vulnerable to exploitation for money laundering purposes considering the difficulties posed to investigating the flow of cash. Nevertheless, there are fewer total cash transactions than purchase & payment transactions, leading to a lower potential consequence of money laundering via ATMs.

D. Terrorist Financing Risk Assessment Analysis

1. Risk Analysis by Region

Terrorist financing risk in the non-bank CBPI sector was assessed by region to ascertain which provinces were most at risk to terrorist financing via non-bank card-based payment instrument issuers. The risk score by region was calculated based on the level of risk in each respective province, measured in accordance with the predetermined risk factors.

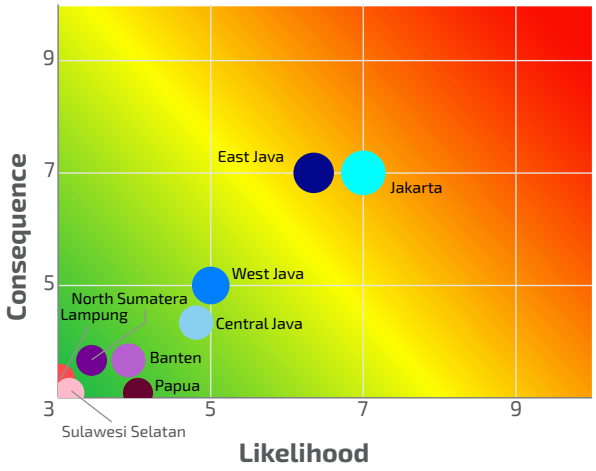
Risk scores were calculated by multiplying the likelihood and consequence for each region or province, while the likelihood was obtained by adding the threat and vulnerability scores. The salient outcomes of the risk analysis by region of terrorist financing in the non-bank CBPI sector are recapitulated in Table 5.6.

Table 5.6. Risk Analysis of Terrorist Financing in Non-Bank CBPI Sector by Province

No	Province	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Jakarta	7,00	7,00	7,00	7,00	**7,00**	Medium
2.	East Java	7,00	7,00	7,00	6,35	**6,22**	Medium
3.	Others	4,88	4,62	5,06	4,71	**4,41**	Low

The results of mapping terrorist financing risk in the non-bank CBPI sector by region is presented in Figure 5.6

Figure 5.6. TF Risk Heatmap by Region in Non-Bank CBPI Sector



Based on the TF risk heatmap presented in Figure 5.6, the provinces with a **medium** level of terrorist financing risk in the non-bank CBPI sector are the **Special Capital Region Jakarta** and **East Java**. All other regions are **low** risk.

Jakarta scored the highest risk scores compared with other provinces. The results of risk assessments conducted by law enforcement agencies and supervisors found that Jakarta and East Java were high-risk regions in terms of terrorist financing through non-bank card-based payment instrument issuers. Furthermore, the high number of non-bank card-based payment instrument transactions in Jakarta increased the potential risk of using card-based payment instruments as a media for terrorist financing.

2. Terrorist Financing Risk based on Individual Customer Profile

Terrorist financing risk was also assessed based on individual customer profile to ascertain which professions were most at risk to financing terrorists in the non-bank CBPI sector.

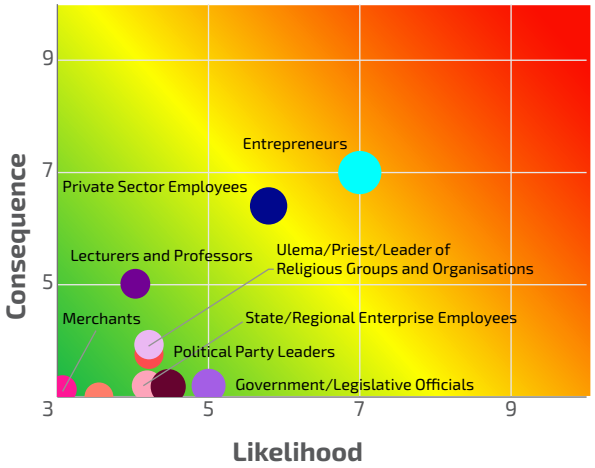
The results of terrorist financing risk analysis in the non-bank CBPI sector based on individual customer profile are presented in Table 5.7.

The results of mapping terrorist financing risk in the non-bank CBPI sector by individual customer profile is presented in Figure 5.7.

Table 5.7. Risk Analysis of Terrorist Financing in Non-Bank CBPI Sector by Individual Customer Profile

No	Profession	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Entrepreneurs	9.00	6.69	7.00	7.00	**7.00**	Medium
2.	Private Sector Employees	6.69	5.04	6.40	5.79	**5.25**	Medium
3.	Others	6.63	4.97	4.44	4.67	**4.13**	Low

Figure 5.7. TF Risk Heatmap by Individual Customer Profile in Non-Bank CBPI Sector



According to the TF risk heatmap presented in Figure 5.7, **Entrepreneurs** and **Private Sector Employees** are medium-risk individual customer profiles in terms of terrorist financing in the non-bank CBPI sector, while other customer profiles are **low** risk. The analysis was based on risk assessments performed by law enforcement agencies, reporting parties and supervisors.

The emerging risk of terrorist financing posed by **Entrepreneurs** is based on court reports showing the involvement of said customer profiles in terrorist financing cases. This was also confirmed by the outcome of the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021, stating that Entrepreneurs were the highest risk customer profile for terrorist financing. Based on an analysis of terrorist financing cases, Entrepreneurs were the dominant customer profile in the form of welding shop owners, herbal medicine sellers and travel agents.

Meanwhile, **Private Sector Employees** are a medium-risk individual customer profile in line with the National Risk Assessment of Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in 2021. Furthermore, Private Sector Employees are the dominant customer profile in the non-bank CBPI sector, thereby increasing the potential risk of terrorist financing.

3. Terrorist Financing Risk based on Products and Services

Terrorist Financing risk was also assessed based on the products and services to ascertain which were most at risk to cases of terrorist financing in the non-bank CBPI sector. The risk analysis based on products and services in the non-bank CBPI sector had the following limitations:

1. In accordance with the authority of Bank Indonesia, AML/CFT policy and supervision only extends to card-based payment instruments issued by non-bank issuers.

2. As the object of this assessment, credit cards are the only product assessed because non-bank card-based payment instrument issuers are not permitted to issue ATM cards or debit cards in Indonesia.

The results of terrorist financing risk analysis in the non-bank CBPI sector based on products and services using several risk factors in the form of risk are presented in Table 5.8.

The results of mapping terrorist financing risk in the non-bank CBPI sector by product and service is presented in Figure 5.8.

According to the TF risk heatmap presented in

Table 5.8. Risk Analysis of Terrorist Financing in Non-Bank CBPI Sector by Product and Service

No	Product and Service	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Purchase and Payment	6.00	4.50	6.00	6.00	**6.00**	Medium
2.	Cash Out	5.00	6.75	5.00	5.00	**5.00**	Low

Figure 5.8. TF Risk Heatmap by Product and Service in Non-Bank CBPI Sector

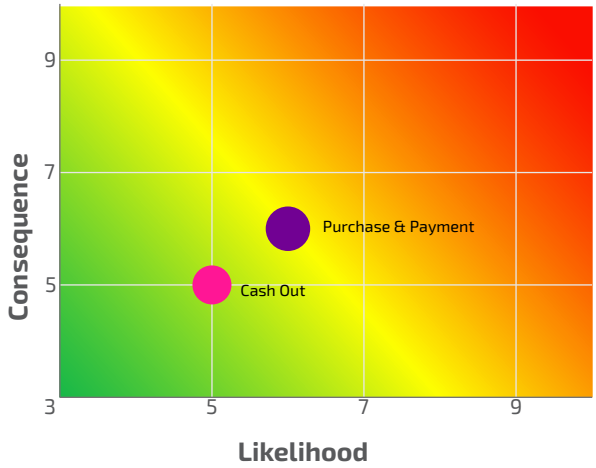


Figure 5.8, **Purchase & Payment** is a **medium-risk** product for terrorist financing in the non-bank CBPI sector, while **Cash Out** is **low** risk.

Fundamentally, the non-bank CBPI sector is vulnerable to misuse as a means of terrorist financing because of the convenient transaction process and difficulties identifying the transacting parties. **Purchase & Payment** is a medium-risk product based on a risk assessment by law enforcement agencies. The threat and consequence scores are high due to the high frequency and value of **Purchase & Payment** transactions in the non-bank CBPI sector. Notwithstanding, the vulnerability of **Purchase & Payment** transactions it is not as high as **Cash Out** because **Purchase & Payment** does not allow the continuous flow of funds and is not as difficult to trace as the **Cash Out** product.

Despite low risk, a risk assessment by law enforcement agencies showed how Cash Out could be used by criminals to conceal funding flows considering how difficult cash is to track and trace. Nevertheless, the low number of Cash Out transactions through the non-bank CBPI sector prompted lower consequence and risk scores for this product/service.

4. Terrorist Financing Risk based on Delivery Channel

Terrorist financing risk was also assessed based on the delivery channel to ascertain which were most at risk to cases of terrorist financing in the non-bank CBPI sector. The delivery channels of non-bank card-based payment instrument issuers are grouped into two main categories, namely delivery channels for the customer registration process and delivery channels for the customers to use the products and services. Customer registration is facilitated by outlets and mobile applications, while the delivery channels for customers to use the products and services include ATMs (for cash withdrawals), offline merchants, online merchants as well as purchase & payment agents.

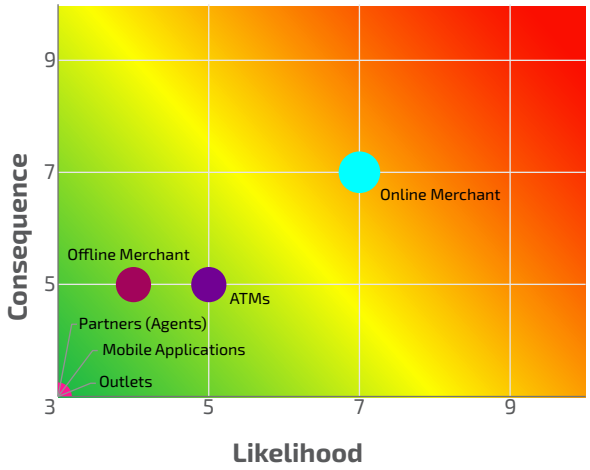
Using risk factors in the form of risk, the level of terrorist financing risk for each delivery channel in the non-bank CBPI sector was assessed and the results are presented in Table 5.9.

The results of mapping terrorist financing risk in the non-bank CBPI sector by delivery channel is presented in Figure 5.9.

Table 5.9. Risk Analysis of Terrorist Financing in Non-Bank CBPI Sector by Delivery Channel

No	Delivery Channel	Threat	Vulnerability	Consequence	Likelihood	Risk Score	Risk Category
1.	Online Merchants	6.50	7.00	7.00	7.00	**7.00**	Medium
2.	Others	5.25	5.25	5.25	5.59	**5.51**	Low

Figure 5.9. TF Risk Heatmap by Delivery Channel in Non-Bank CBPI Sector



According to the TF risk heatmap presented in Figure 5.9, **Online Merchants** are a **high-risk** delivery channel for terrorist financing in the non-bank CBPI sector, while all other delivery channels are **low** risk.

Based on a risk assessment by law enforcement agencies, **Online Merchants** are a **medium-risk** delivery channel for terrorist financing in the non-bank CBPI sector. In terms of the threats and consequences, **Online Merchants** received medium scores, along with a high vulnerability score. Furthermore, a shift has occurred from cash to cashless transactions in response to the Covid-19 pandemic, thereby significantly increasing online credit card transactions and increasing the potential risks as a means of terrorist financing.

3

RISK MITIGATION

A. Institutional Aspects of Risk Mitigation

Referring to the Bank Indonesia Regulation (PBI) on Card-Based Payment Instruments and External Circular Letter on Card-Based Payment Instruments, the following institutional mitigation measures are taken:

1. Non-bank Card-Based Payment Instrument (CBPI) in Indonesia must be licensed by Bank Indonesia.

2. Management and shareholders of non-bank card-based payment instrument issuers are required to meet the following requirements set by Bank Indonesia:

    a. Not included on the National Blacklist (DHN)[51] for withdrawals of blank cheques and/or money transfers.

    b. Not convicted of a crime in the last two years.

    c. Fulfilled tax obligations.

    d. No bad loans.

    e. Not declared bankrupt in the two years prior to application.

6. Paid-up capital in non-bank card-based payment instrument issuers cannot be obtained from and/or used for money laundering.

7. Non-bank card-based payment instrument issuers are required to fulfil regular and special reporting obligations to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

8. Non-bank card-based payment instrument issuers are not permitted to issue Credit Cards or Debit Cards.

9. When processing the CBPI license, Bank Indonesia will perform background checks on the applicant, including confirmation or requests for information to other relevant authorities and organisations.

The latest PJP regulations contain the following mitigation measures:

1. At least 15% of the shareholdings of non-bank card-based payment instrument issuers must be owned by Indonesian citizens and/or Indonesian business entities, and at least 51% of the shares with voting rights must be owned by Indonesian citizens and/or Indonesian business entities.

2. Bank Indonesia may determine the validity period of a PJP licence as required based on licence category, business activity and/or the source of funding.

3. Bank Indonesia will evaluate the PJP licence every three years or incidentally as required.

B. Operational Aspects of Risk Mitigation

a. Pre-Transaction Mitigation Measures

1. Non-bank card-based payment instrument issuers implement an AML/CFT program for the operating activities as follows:

    a. Roles and responsibilities of the Directors and active supervision of the Board of Commissioners.

51 In accordance with Bank Indonesia Regulation (PBI) No. 8/29/PBI/2006 concerning the National Blacklist for Withdrawals of Blank Cheques and/or Money Transfers, persons drawing blank cheques and/or money transfers will be listed on the National Blacklist set by Bank Indonesia.

b. Policies and written procedures.

c. Risk management process.

d. Management of human resources.

e. Internal control system.

2. Restrictions on Credit Card facilities available to customers based on income. Customers with monthly income of less than Rp3 million are not eligible for credit card facilities, while customers with monthly income of Rp3-10 million are eligible for one credit card facility. Customers with monthly income of more than Rp10 million are eligible for more than three credit card facilities.

3. Issuing credit card facilities to a prospective customer who already has credit card facilities issued by another bank as a source of customer profile information, including occupation, address, payslip, income and tax file number.

4. Non-bank card-based payment instrument issuers are required to implement Customer Due Diligence (CDD), namely the identification and verification of customers, including the legal arrangements, nominees and/or Beneficial Owners.

5. In terms of identification and verification of the Beneficial Owner, enhanced due diligence is required of the following:

   a. Additional credit card for the main credit card facility, such as an additional credit card used by a family member.

   b. Potential use by a third party of a credit card issued to a customer.

6. For application-based CDD, non-bank card-based payment instrument issuers are recommended to deploy liveness detection features. In addition, the non-face-to-face verification process must be supported by various other efforts performed by independent and credible sources, including tracking the internet protocol (IP) address of customers and seeking information on prospective customers from various credible sources.

7. Non-bank card-based payment instrument issuers administrate, update and confirm the accuracy of customer information, particularly high-risk customer profiles.

8. Non-bank card-based payment instrument issuers have access to various independent and reliable sources of data to verify customer profiles, including data from the Directorate General of Population and Civil Registration of Indonesia, as well as access to international databases, such as World-Check.

9. Non-bank card-based payment instrument issuers have access to the database of Politically Exposed Persons (PEP) administrated by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

10. Enhanced Due Diligence (EDD) is required for high-risk customer profiles.

11. Non-bank card-based payment instrument issuers are obliged to update and exchange information concerning the Credit Card Blacklist.

12. When cooperating with a third party, non-bank card-based payment instrument issuers ensure adequate AML/CFT implementation by the third party, including CDD based on FATF Recommendation 17.

The latest PJP regulations also contain the following additional mitigation measures in terms of credit risk management:

1. Minimum age of cardholder.
2. Minimum income of cardholder.
3. Maximum credit ceiling available to cardholder.
4. Maximum number of PJP administrating funding sources in the form of issuing credit cards.
5. Minimum payment by cardholdert.

b. Transaction Mitigation Measures

1. Restrictions on several credit card features, for example the cash out facility is restricted to 40-60% of the overall credit ceiling. In addition, non-bank card-based payment instrument issuers have discretion to set a daily cash withdrawal limit.
2. Cash withdrawals using Credit Cards are only available via ATM machines using a Personal Identification Number (PIN). There are two security elements, namely CCTV around the ATM and the PIN that is only known to the cardholder.
3. For online e-commerce purchases using credit cards, transaction authorisation is achieved using static and dynamic data known only to the cardholder. Payment security (payment transactions) is the responsibility of both parties, namely the credit card issuer and the e-commerce platform, while security of purchased goods (purchase transactions) is the responsibility of the e-commerce platform.
4. All non-bank card-based payment instrument issuers are connected to the AKKI[52] system, which can monitor customer profiles and transaction profiles as well as customer profile history.
5. Non-bank card-based payment instrument issuers can impose limits on credit card payment transactions through agents or third parties in the context of risk management.

c. Post-Transaction Mitigation Measures

1. Non-bank card-based payment instrument issuers manage data, information and documents as well as monitor transactions, which includes updating customer profiles and customer transaction profiles.
2. Non-bank card-based payment instrument issuers deploy a Fraud Detection System (FDS) to identify and red flag indications of fraud or unusual transactions. FDS is expected to detect fraud referring to a typology database, identify high-risk customer profiles and transactions as well as detect simultaneous transactions by multiple accounts and at multiple merchants.
3. Non-bank card-based payment instrument issuers identify and report suspicious transactions to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC).

According to the provisions contained in the latest PJP regulations, the additional mitigation measures include obligations to enhance security standards for specific transactions by providing transaction alerts for credit card customers through media agreed by the cardholder and/or other security standards.

d. Additional Risk Mitigation Measures relating to Terrorist Financing

a. Non-bank card-based payment instrument issuers block or freeze funds belonging to individuals or corporations identified on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).

b. Non-bank card-based payment instrument issuers conduct rigorous investigations concerning the modus operandi and

52 The Indonesia Credit Card Association (AKKI) is an organisation of credit card issuers as a partner of the regulator to increase convenience and security for credit card users.

typologies of terrorist financing cases used by terrorist groups for more effective preventative measures.

c. Non-bank card-based payment instrument issuers administrate and update the List of Suspected Terrorists and Terrorist Organisations (DTTOT) and relevant UN Security Council Resolutions based on automatic screening to mitigate terrorist financing.

d. Non-bank card-based payment instrument issuers subscribe to international databases, such as World-Check, in relation to Politically Exposed Persons (PEP) and the List of Suspected Terrorists and Terrorist Organisations (DTTOT) in order to mitigate terrorist financing.

e. Non-bank card-based payment instrument issuers implement enhanced due diligence for high-risk prospective customers, customers or beneficial owners to mitigate the exploitation of immediate family members, including wives, children and others, to finance terrorism.

f. In terms of collaborating with third parties, such as agents or partners, non-bank card-based payment instrument issuers ensure adequate AML/CFT implementation by the third party.

C. Supervision Aspects of Risk Mitigation

1. Bank Indonesia applies risk-based supervision to AML/CFT implementation by non-bank card-based payment instrument issuers within a supervision cycle of direct and indirect supervision, inspections, evaluations and follow-up actions. Evaluations and follow-up actions are forms of indirect supervision based on the results of inspections as well as training and/or the imposition of sanctions.

2. Bank Indonesia performs thematic supervision of non-bank card-based payment instrument issuers.

3. Bank Indonesia may assign other parties for and on behalf of Bank Indonesia to perform inspections of non-bank card-based payment instrument issuers.

4. Concerning supervision by Bank Indonesia, non-bank card-based payment instrument issuers identify, manage and update data concerning the Beneficial Owners, while ensuring the availability of data on Beneficial Owners in the interest of Bank Indonesia supervision.

5. Bank Indonesia regulates cashback practices in cooperation with the National Police of the Republic of Indonesia.

4

CONCLUSIONS

A. Money Laundering Risks

Based on the outcome of statistical data analysis and the risk score of sectoral money laundering in the non-bank CBPI sector by **region (province), customer profile, product** and **service** as well as **delivery channel**, the following conclusions were drawn:

1. The **Special Capital Region of Jakarta** is a **high-risk** region for money laundering activity in the non-bank CBPI sector, followed by the provinces of **West Java** and **East Java** as **medium-risk** regions. All other provinces are **low** risk.

2. **Politically Exposed Persons (PEP)** are a **high-risk** individual customer profile for money laundering activity in the non-bank CBPI sector, followed **Entrepreneurs** as **medium** risk. All other individual customer profiles are **low** risk.

3. **Government Institutions** and **Non-MSME Limited Liability Companies (PT)** are **medium-risk** institutional customer profiles for money laundering activity in the non-bank CBPI sector. All other institutional customer profiles are **low** risk.

4. **Purchase & Payment** is a **medium-risk** product concerning money laundering activity in the non-bank CBPI sector. All other products and services are **low** risk.

5. **Online Merchants** and **ATMs** are **medium-risk** delivery channels concerning money laundering activity in the non-bank CBPI sector. All other delivery channels are **low** risk.

Table 5.10. Outcome of Sectoral Risk Assessment of Money Laundering in Non-Bank CBPI Sector

Risk	Province	Profession	Business Entity	Product/Service	Delivery Channel
High	Jakarta	PEPs	-	-	-
Medium	West Java, East Java	Entrepreneurs	Government Institutions, Non-MSME Limited Liability Companies (PT)	Purchase/Payment	Online Merchants, ATMS
Low	Others	Others	Others	Cash Out	Others

B. Terrorist Financing Risk

Based on the latest assessment, the level of terrorist financing risk in the non-bank CBPI sector by **region (province), customer profile, product** and **service** as well as **delivery channel** is as follows:

1. The **Special Capital Region of Jakarta** and **East Java** are **medium-risk** regions for terrorist financing activity in the non-bank CBPI sector. All other provinces are **low** risk.
2. **Entrepreneurs** and **Private Sector Employees** are **medium-risk** individual customer profiles for terrorist financing activity in the non-bank CBPI sector. All other individual customer profiles are **low** risk.
3. **Purchase & Payment** is a **medium-risk** product for terrorist financing activity in the non-bank CBPI sector. All other products and services are **low** risk.
4. **Online Merchants** are a **medium-risk** delivery channel for terrorist financing activity in the non-bank CBPI sector. All other delivery channels are **low** risk.

Table 5.11. Outcome of Sectoral Risk Assessment of Terrorist Financing in Non-Bank CBPI Sector

Risk	Province	Profession	Product/Service	Delivery Channel
High	-	-	-	-
Medium	Jakarta, East Java	Entrepreneurs, Private Sector Employees	Purchase/Payment	Online Merchants
Low	Others	Others	Cash Out	Others

PART III

1

FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

A. Proliferation Financing Risk Landscape

Based on the National Risk Assessment of Financing of Proliferation of Weapons of Mass Destruction (WMD) in 2021, the emerging threats posed by proliferation financing Indonesia stem from the following:

1. Trade finance between parties from high-risk countries based on UN Security Council Resolution.
2. Misuse of accounts belonging to non-residents from high-risk countries based on UN Security Council Resolution who no longer live/work in Indonesia.

Based on the emerging risks, a number of risk mitigation measures to counter proliferation financing are required as follows:

1. Intensive surveillance is required of nationals from countries sanctioned by the United Nations Security Council who stay or have stayed in Indonesia, primarily to detect direct or indirect transactions or activities involving sanctioned individuals, entities, states or regions.
2. Expunge the account data for foreign diplomats, particularly from North Korea and Iran, who are no longer actively serving in Indonesia.

There have been no significant cases relating to proliferation financing identified in Indonesia but the potential risks must still be anticipated together with the evolution of methods used by criminals to disguise the funding activities employed for the development and use of nuclear, chemical, radiological and biological weapons, as well as the wider distribution of operational areas for WMD development to various jurisdictions.

Based on the analysis, general proliferation financing activities consist of the following:

1. Operating globally and exploiting countries with weak export and financial controls.
2. Using formal financial systems, yet also using informal systems and cash.
3. Purchasing proliferation sensitive goods through the open market.
4. Using shell companies and trade intermediaries to conceal the end use and end users.

Based on the FATF Guidance on Proliferation Financing Risk Assessment and Mitigation published in June 2021, there are several proliferation financing risk indicators in the customer profile as follows:

1. Customer is reluctant to provide additional information about their activities.
2. During subsequent stages of due diligence, a customer, particularly a trade entity, its owners or senior managers, appear in sanctioned lists concerning proliferation financing.
3. The customer is a person connected with a country of proliferation concern or sanctioned by the UN Security Council based on the latest credible and independent information, including the National Risk Assessment.
4. The customer is a person dealing with dual-use goods, goods subject to export control, or complex equipment for which he/she lacks technical background, or which is incongruent with their customer profile.
5. A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with the stated business profile.

6. A customer conducts rapid movement high-volume transactions without clear business reasons. In some cases, the activity of transferring funds is done by business entities that may be connected to a state-sponsored proliferation program, and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.

7. A customer affiliated with a university or research institution is involved in the trading of dual use goods or goods subject to export control.

Meanwhile, the following account and transaction activity risk indicators have also been identified:

1. The originator and/or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern based on the latest sources of credible and independent information, including the National Risk Assessment, or a country sanctioned by the UN Security Council.

2. Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes.

3. Accounts or transactions involve companies with opaque ownership structures, front companies or shell companies.

4. Demonstrating links between representatives of companies exchanging goods, such as same owners or management, same physical address, IP address or telephone number, or their business activities may be coordinated.

5. Account holder conducts financial transactions in a circuitous manner.

6. Account activity or transactions where the originator or beneficiary of associated financial institutions or branches is domiciled in a country with weak implementation of relevant UN Security Council obligations or high risk of proliferation financing based on the latest credible and independent sources of information, including the National Risk Assessment.

7. Trade transactions using cash.

In addition, the products and services vulnerable to exploitation as a means of proliferation financing include those products and services that facilitate cross-border transactions and/or products and services accessible in different jurisdictions. Meanwhile, delivery channel risk must be considered by payment service providers (PJP) with branches and/or agents in different jurisdictions.

Based on the literature, several proliferation financing typologies have been identified as follows:

1. Transactions using false identity documents.
2. Transactions using fictitious or invalid documents.
3. Transactions incongruent with customer profile.
4. Transactions using fictitious information concerning delivery location.
5. Customers providing invalid information, particularly concerning the goods or services exported.
6. Transactions without supporting documents, such as trade documents, etc.
7. Customers failing to provide clear and valid information and reluctant to disclose additional information.
8. Money transfer transactions followed immediately by cash withdrawals.
9. Transactions using private or corporate accounts.
10. Use of shell companies.
11. Use of front companies.
12. Transactions involving countries vulnerable to proliferation activities.
13. Transactions involving foreign individuals or entities to conceal the flow of funds.

14. Transactions involving freight forwarders.
15. Transactions involving exporters-importers.
16. Order transactions for goods initiated by foreign individuals or companies.
17. Transactions involving the delivery of goods incongruent with the country profile. For instance, sending semiconductor manufacturing equipment to a country without an electronics industry.
18. There is a connection between businesses sending goods to each other, namely the same owner or management.
19. Circuitous shipping routes.
20. Transactions involving shipping routes to countries with weak export-import laws.
21. Transactions involving the delivery of goods incongruent with established trade patterns.
22. Transactions involving financial institutions with weak AML/CFT supervision or countries with weak AML/CFT regimes.
23. Transactions with low shipping costs.
24. Inconsistent information between financial documents and financial flows.
25. Transactions using wire transfers.
26. Unusual wire transfer activity without a clear destination.
27. New customers requesting letters of credit.
28. Payment instruction from or to parties not named in the documentation.
29. Transactions involving controlled goods under a WMD export control regime.
30. Transactions involving individuals or entities connected to countries vulnerable to proliferation financing practices.
31. Transactions involving individuals or entities from countries vulnerable to proliferation financing practices.
32. Transactions using cash or precious metals.
33. Involvement of small trading companies or intermediaries conducting business activity incongruent with stated business activity.
34. Companies initiating illegal money transfers.
35. Inter-affiliate transactions.
36. Demonstrating links between customers and partners, such as the same address, IP address or telephone number.
37. Transactions involving universities in countries vulnerable to proliferation practices.
38. Purchasing industrial or commercial goods using private accounts.
39. Customers included on sanctioned lists or blocked from export activity.
40. Customers involved in complex trade transactions, involving numerous intermediaries and third parties in business activities incongruent with the business profile.
41. Beneficial owner domiciled in countries vulnerable to proliferation practices.
42. Transactions using or involving companies with ambiguous ownership structure.
43. Transactions using cash performed by manufacturing companies or trading companies.
44. Transactions with a different delivery destination to the location of the importer.
45. Import payment transactions performed by another entity.

B. Proliferation Financing Risk Analysis in Non-Bank Payment Service Providers and Non-Bank Money Changers

Based on a risk assessment performed by PJP, no customer profiles, business entities, products or delivery channels have been identified as high risk of financing of proliferation of weapons of mass destruction. Notwithstanding, the customer profiles most at risk of proliferation financing are management/employees of non-governmental organisations (NGOs), politically exposed persons (PEPs) and entrepreneurs. Entrepreneurs are considered higher risk in line with the results of an FATF assessment, showing that proliferation financing relates closely with import-export

activities, especially industries that produce dual-use goods. In terms of corporate customer profile, non-MSME limited liability companies (PT) have the highest potential proliferation risk compared with other corporate profiles. In the context of products and services, the potential risk of proliferation financing is highest for USD and SGD using a cash-based foreign currency purchase-selling mechanism in non-bank money changers, as well as cash-to-cash products, including outgoing, incoming and domestic transactions via non-bank Money or Value Transfer Services (MVTS).

C. Proliferation Financing Risk Mitigation

In addition to the money laundering and terrorist financing risk mitigation measures mentioned previously, the following proliferation financing risk mitigation measures are available:

1. Non-bank payment service providers and non-bank money changers block or freeze funds belonging to individuals or corporations identified on the Proliferation Financing List.

2. Non-bank payment service providers and non-bank money changers conduct rigorous investigations concerning the modus operandi and typologies of proliferation financing cases for more effective preventative measures.

3. Non-bank payment service providers and non-bank money changers administrate and update the List of Proliferation Financing as well as the FATF List of High-Risk Jurisdictions Subject to a Call for Action[53] and Jurisdictions Under Increased Monitoring[54] based on automatic screening to mitigate proliferation financing of WMD.

4. Non-bank payment service providers and non-bank money changers subscribe to international databases, such as World-Check, in relation to Proliferation Financing in order to mitigate proliferation financing of WMD.

5. Non-bank payment service providers and non-bank money changers implement enhanced due diligence for high-risk prospective customers, customers or beneficial owners to mitigate the exploitation of immediate family members, including wives, children and others, to finance proliferation.

6. In terms of collaborating with third parties, such as agents or partners, non-bank payment service providers and non-bank money changers ensure adequate AML/CFT implementation by the third party.

53 High-Risk Jurisdictions Subject to a Call for Action identifies and blacklists countries or jurisdictions with serious strategic deficiencies to counter cases of money laundering, terrorist financing and proliferation.

54 Jurisdictions Under Increased Monitoring are countries that have committed to resolve swiftly the identified strategic deficiencies in the money laundering, terrorist financing and proliferation financing regime within agreed timeframes. This list is often externally referred to as the grey list.


+1583
+31
+1251

PART IV

1

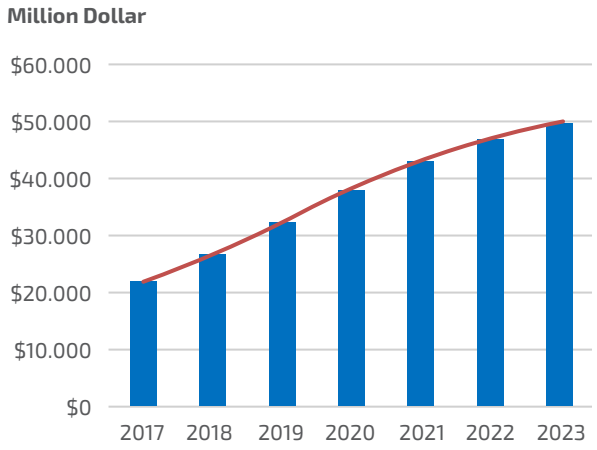
EMERGING RISKS DURING COVID-19 PANDEMIC

A. Emerging Risks of Money Laundering During Covid-19 Pandemic

Since the beginning of 2020, the coronavirus disease 2019 (Covid-19) pandemic has spread rapidly around the world, bringing high infection and fatality rates. In addition to triggering a health crisis, the Covid-19 pandemic has also had a significant impact on socio-economic and financial conditions. Indonesia is one of many countries affected by the Covid-19 outbreak. The socio-economic impact has been felt through social restrictions/lockdown, higher unemployment and sluggish economic performance, the reprioritisation of government programs and resources to handle the Covid-19 pandemic, a dramatic increase in online sales and higher demand for medical equipment, among others.

On the other hand, the Covid-19 pandemic has accelerated digital adoption in Indonesia, digital payments in particular. Based on the Statista Digital Market Outlook (2020), Indonesia has experienced an increase in transaction volume using digital payments. In September 2021, Bank Indonesia recorded 470 million transactions worth Rp27.6 trillion using electronic money, increasing 28% and 56.3% respectively compared with conditions in September 2020. Furthermore, the Covid-19 pandemic has also compelled non-bank payment service providers and non-bank money changers to become more innovative in terms of using digital-based transactions to reduce the risk of transmitting Covid-19.

Graph 7.1. Digital Payments in Indonesia



Source: Digital Market Outlook, Statista (2020)

A special study conducted by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) concerning money laundering risk in relation to the Covid-19 pandemic in 2020 found that 14% of reporting parties, including non-bank payment service providers and non-bank money changers, did not offer any form of face-to-face services. The INTRAC study also revealed the estimated proportion of transactions through digital services compared to total transactions during the Covid-19 pandemic, with digital transaction volume dominating 72% and digital transaction value 61%.

The growing use of digital transaction services, however, poses a money laundering risk. As stated by the FATF President in 2020[55], the risk of money laundering and terrorist financing is increasing due to the Covid-19 pandemic. According to the FATF report on Covid-19-related Money Laundering and Terrorist Financing - Risk and Policy Responses (May 2020), the emerging threat of money laundering relates to the misuse

55 Statement of FATF President on 23rd October 2020 relating to the Covid-19 pandemic: https://www.fatf-gafi.org/publications/COVID-19/COVID-19.html?hf=10&b=0&s=desc(fatf_releasedate)

of online financial services and virtual assets to move and conceal illicit funds, misuse and misappropriation of domestic and international financial aid and emergency funding to overcome the Covid-19 impact, impersonation of government officials, counterfeiting of essential goods such as medical supplies and medicines, fundraising for fake charities and fraudulent investment scams. In terms of cybercrime, the threats include email attacks and SMS phishing, business email compromise scams and ransomware attacks. The results of a global crime threat assessment by the International Criminal Police Organisation (Interpol) in 2020 also demonstrated an increase in digital threats linked to malicious domains, malware and ransomware.

According to the same study conducted by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) concerning money laundering risk in relation to the Covid-19 pandemic in 2020, the risk of money laundering based on the predicate offences of fraud, corruption, narcotics and illicit money transfers has increased during the Covid-19 pandemic. A paradigm shift in consumer behaviour among Indonesians towards greater use of e-commerce and growing demand for medical equipment have been exploited by criminals. The Indonesian police has recorded the highest number of online fraud cases reported during the Covid-19 pandemic. In addition, the pandemic has exposed several vulnerabilities that have been exploited through corruption, including goods and services procurement, state and regional budget allocation as well as third-party donations. Narcotics criminals have also exploited technology, with the number of narcotics cases also increasing during the Covid-19 pandemic. Meanwhile, higher demand for medical equipment globally and the use of digital-based transaction services are also being exploited by online criminals to transfer funds in relation to business email compromise (BEC).

Change in Money Laundering Risk Landscape during Covid-19 Pandemic

In response to lockdown policy instituted in numerous jurisdictions and large-scale social restrictions in Indonesia, transaction volume, particularly at non-bank money changers (KUPVA) and non-bank Money or Value Transfer Services (MVTS), has fallen precipitously. In contrast, the volume of electronic money transactions has trended upwards, especially since Quick Response Code Indonesia Standard (QRIS) implementation launched at the beginning of 2020. Most Indonesians are transitioning towards cashless transactions to help break the domestic chain of Covid-19 transmission. Furthermore, the Government has also turned to cashless social aid program (bansos) disbursements using electronic money after the Government selected an e-money issuer as partner.

According to a survey of non-bank payment service providers and non-bank money changers under the regulatory and supervisory jurisdiction of Bank Indonesia conducted by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), the number of red flag alerts concerning money laundering has declined during the Covid-19 pandemic (as of October 2020) compared with the pre-pandemic period. During the same period, a trend of suspicious transactions has emerged, including the use of false ID documents during the customer due diligence process, cashback abuse by criminals at merchants using electronic money, the use of counterfeit foreign banknotes in non-bank money changers, customer profile fraud in the name of the electronic money issuer and fundraising via online platforms under the pretence of donations.

B. Emerging Risk of Terrorist Financing During Covid-19 Pandemic

According to the Impact of the Covid-19 Pandemic on Terrorism, Counter-Terrorism and Countering Violent Extremism published in June 2021 by the United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), the Covid-19 pandemic has exposed a number of short-term vulnerabilities. The short-term vulnerabilities include greater internet use amongst students and exploiting the government's focus on pandemic mitigation measures by terrorist groups. The update of the CTED report in 2021 also stated that the social, economic and political impact of the Covid-19 pandemic will increase terrorism risk moving forward. The Covid-19 pandemic has been shown to pose various counter-terrorism challenges due to the reallocation of counter-terrorism resources and budgets in several jurisdictions. Based on the FATF report on Covid-19-related Money Laundering and Terrorist Financing - Risk and Policy Responses (May 2020), the emerging terrorist financing threats relate to the risks associated with collecting illicit funds and using false charity organisations to collect and transfer funds used for terrorist acts.

Terrorist groups are known to have remained active during the pandemic using technological advances. The National Counter-Terrorism Agency (BNPT) stated that terrorist networks have continued to recruit new members through online media by spreading ideas of terrorism, intolerance and radicalism during the pandemic. Terrorist groups also use online media for fundraising purposes. The Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) recorded 24 analysis results relating to alleged criminal acts of terrorist financing in 2020 (as of June).

Change in Terrorist Financing Risk Landscape during Covid-19 Pandemic

Based on the 2020 CTED report, a number of new short-term risks have emerged due to the Covid-19 pandemic. Restrictions on international travel and increased border security have impacted the movement of terrorist groups, particularly foreign terrorist fighters (FTFs). In addition, social restrictions have made it more difficult for terrorists in remote areas to access basic commodities.

According to a survey of non-bank payment service providers and non-bank money changers under the regulatory and supervisory jurisdiction of Bank Indonesia conducted by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), the number of red flag alerts concerning terrorist financing has declined during the Covid-19 pandemic (as of October 2020) compared with the pre-pandemic period.

Notwithstanding, potential risks and emerging threats relating to terrorist financing and financing of proliferation of weapons of mass destruction have increased in line with the rapid growth of cashless transactions. Based on a self-assessment performed by non-bank payment service providers and non-bank money changers regarding the Covid-19 pandemic impact, the potential risk of terrorist financing through the following typologies have been identified:

a. Fundraising activities through private donations, community organisations, independent funding, legal businesses and social media.

b. Money transfers via financial services providers, cross-border cash carriers, trade of goods and services, new payment methods and through different professions.

c. Using funds for terrorist operations, member salaries and compensation, recruitment and propaganda, health services, education, social benefits and training.

C. Challenges During Covid-19 Pandemic

The challenges faced by non-bank payment service providers and non-bank money changers in terms of implementing AML/CFT programs during the Covid-19 pandemic were largely influenced by operational restrictions due to the suspension of business activities and introduction of work from home (WFH) protocols. A portion of non-bank payment service providers and non-bank money changers opted to close operational activities temporarily during the large-scale social restrictions and travel restrictions. In addition, constraints were also faced when implementing split operation WFH, including limited access to databases maintained by the Directorate General of Population and Civil Records of Indonesia as well as the Legal Entity Administration System for the customer verification process and electronic customer due diligence (e-CDD).

Notwithstanding, based on a survey of non-bank payment service providers and non-bank money changers conducted by Bank Indonesia, AML/CFT Compliance Units have maintained optimal tasks and functions throughout the pandemic since March 2020. As follow-up actions and risk mitigation measures against money laundering, non-bank payment service providers and non-bank money changers have prepared case studies and investigated suspicious transactions, implemented enhanced due diligence (EDD) and reported suspicious transactions to the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), rejected customers based on the accuracy of identification documents, updated the blacklist maintained by law enforcement agencies, continued to coordinate with Bank Indonesia as a supervisory and regulatory body (LPP) and INTRAC to mitigate money laundering risk during the pandemic and implemented enhanced due diligence with additional indicators relevant to customer profile risk. Non-bank payment service providers and non-bank money changers have also introduced various innovations, including the application of regulatory technology (RegTech) in the AML/CFT compliance program, refined the fraud detection system (FDS) well as used internal systems and/or applications to detect suspicious transactions and monitor customer transactions.

D. Bank Indonesia Policy Response to Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) During Covid-19 Pandemic

Bank Indonesia has implemented several policy responses to the Covid-19 pandemic to support contactless transactions by accelerating the uptake of digital transactions. As a supervisory and regulatory body (LPP) for the payment system, Bank Indonesia promulgated Bank Indonesia Regulation (PBI) No. 22/7/PBI/2020 as an amendment to the implementation of several Bank Indonesia regulations impacted by the Covid-19 pandemic, and Board of Governors Regulation (PADG) No. 22/3/PDG/2020 concerning Governance in Task Implementation Continuity at Bank Indonesia during National Disaster and Covid-19 Pandemic Status. Furthermore, Bank Indonesia has also delivered four relevant outputs as follows:

a. An appeal to increase vigilance at non-bank payment service providers and non-bank money changers in anticipation of a potential increase of money laundering, terrorist financing and other financial crimes during the pandemic.

b. Inspection guidelines for supervisors to implement planned audits remotely under specific conditions. The scope of the guidelines covers inspections of AML/CFT and other risks to optimise the implementation of Bank Indonesia's supervisory duties during the enforcement of large-scale social restrictions (social distancing).

c. Guidance on Customer Due Diligence (CDD), including guidelines on electronic customer due diligence (e-CDD), for broader adoption of digital payments.

d. Digital signature policy for credit card customer onboarding to increase adoption of digital payments.

2

EMERGING THREATS OF MONEY LAUNDERING, TERRORIST FINANCING AND FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION IN INDONESIA

Based on the national risk assessment of money laundering and terrorist financing in 2021 and surveys conducted by Bank Indonesia, several typologies of money laundering and terrorist financing were identified with the potential to develop into an emerging threat as follows:

1. **Use of Virtual Currency**

   The National Risk Assessment performed in 2015 identified virtual currency as an emerging threat in Indonesia in line with rapid growth of virtual currency as a payment instrument in Indonesia. In addition, bitcoin ATMs were also installed at several locations in Indonesia.

   Virtual currency poses an emerging threat in terms of money laundering and terrorist financing due to the characteristics of cryptocurrency, which is recognised globally and can be used for cross-border transactions, while not requiring original identification documents. Criminals can exploit virtual currency as a medium for transferring illicit funds from the proceeds of crime or to fund terrorist activities. Furthermore, the FATF Guidance on Proliferation Financing Risk Assessment and Mitigation published in June 2021 found that individuals and/or entities involved in proliferation financing and/or identified on the proliferation financing list favour virtual assets because access to formal products and services from banks and/or non-bank payment service providers has been restricted.

   Mitigating the risks associated with using virtual currency, Bank Indonesia has explicitly forbidden all non-bank payment service providers from receiving, using, connecting and/or processing payment transactions using virtual currency. Additionally, Bank Indonesia takes firm action against PJPs under the supervision and regulation of Bank Indonesia who are shown to have received, used, connected and/or processed payment transactions currency.

2. **Terrorist Financing by Business Entities (Corporations)**

   Terrorist financing by terrorist groups via business entities must be taken into consideration. Terrorist groups can use business entities to collect funds through legal and illegal business activities. Using legal business activities, terrorist groups can access formal products and services provided by the banking industry and non-bank payment service providers to collect, transfer and use funds as if conducting regular business transactions.

   Based on a survey conducted by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), non-MSME limited liability companies (PT) and limited partnership companies (CV) are the customer profiles most at risk of terrorist financing. Seeking to mitigate the emerging threats of terrorist financing by corporate customers, non-bank payment service providers are required to implement enhanced due diligence and monitor the business transactions of such high-risk customer profiles. Several risk indicators of proliferation financing among corporate customers have been identified as follows:

a. Business transactions with parties domiciled in or originating from conflict zones and/or surrounding regions.

b. Customers who are unable and/or unwilling to provide complete documentation and/or additional information concerning the proposed business activity.

3. Buying and selling practices and use of third-party accounts by crime syndicates

The buying and selling practices and use of third-party accounts by crime syndicates include the following activities:

a. Syndicates seeking third-party accounts for subsequent sale to criminals as required.

b. The sale of accounts independently for economic reasons.

c. Syndicates using social engineering and money mule networks.

4. Misuse of e-commerce in transactions using the illicit proceeds of crime.

Potential money laundering activities via e-commerce can occur under the following circumstances:

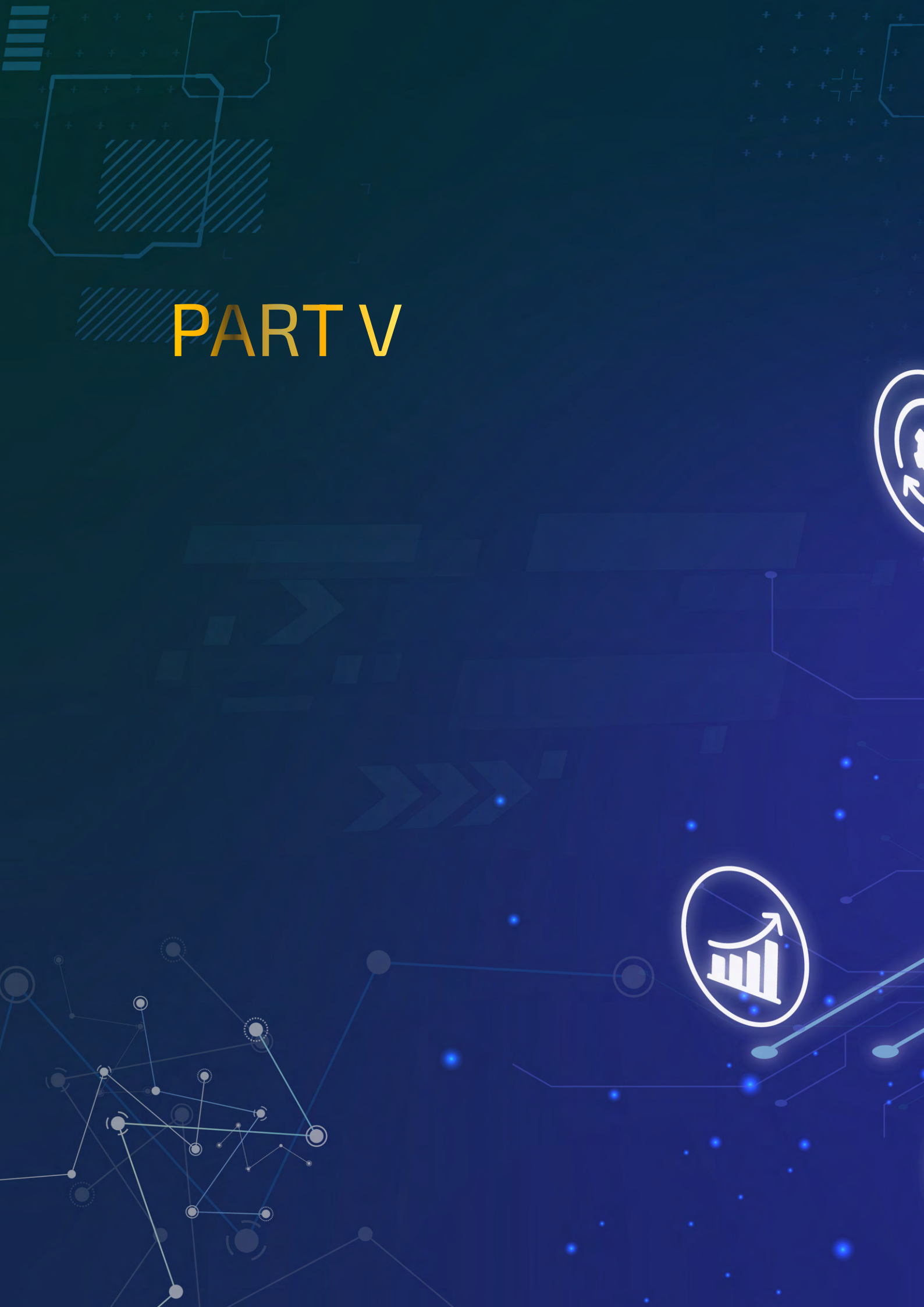
a. Use of e-commerce platforms for bribery purposes through the purchase of high-end or luxury goods.

b. Purchase of high-end goods or services (travel or accommodation) via a merchant purely for money transfer purposes without receiving the goods or services ordered.

c. Exploiting e-commerce platforms with limitations/weaknesses in the identification process concerning the originator name to transact goods and services.

d. Illegal cross-border e-commerce practices or illegal imports via e-commerce platforms pose a criminal threat and incur state losses.

PART V




INTEGRITY
SECURITY
GROWTH
RELIABILITY
STABILITY

RECOMMENDATIONS

A. Recommendations for Bank Indonesia

Based on analysis of the threats, vulnerabilities and consequences, as well as risk assessments concerning money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank payment service providers and non-bank money changers, the following recommendations apply to Bank Indonesia as a supervisory and regulatory body (LPP):

1. Adopting the outcomes of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA) of the payment system to update and increase risk mitigation measures against money laundering, terrorist financing and proliferation financing in the supervision process.
2. Disseminating the outcomes of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA) to employees in the payment system sector, particularly those handling regulation, licensing and supervision, to strengthen a risk-based approach to anti-money laundering and combating the financing of terrorism (AML/CFT).
3. Implementing regular capacity building, specifically targeting employees responsible for supervision, to increase awareness of anti-money laundering and combating the financing of terrorism (AML/CFT).
4. Disseminating the outcomes of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA) to the public to raise awareness concerning the risks associated with money laundering, terrorist financing and proliferation financing in the payment system, particularly focusing on illegal providers.
5. Enhancing the quality of risk-based supervision through supervisory technology (SupTech).
6. Strengthening institutional coordination and cooperation with other relevant authorities and organisations domestically and internationally in terms of:
    a. Compiling a joint watchlist between government ministries/agencies and service providers to mitigate money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.
    b. Compiling and sharing known typologies of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction between government ministries/agencies and service providers as a reference for the implementation of red flag alerts on customer transactions.
    c. Redoubling efforts to control unlicensed non-bank money changers and illegal non-bank payment service providers.
    d. Optimising Public Private Partnerships (PPP) when compiling the watchlist and typologies list, and when controlling unlicensed non-bank money changers and illegal non-bank payment service providers.
7. Implementing public campaigns concerning the importance of anti-money laundering and combating the financing of terrorism (AML/CFT), along with the negative economic impact of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

B. Recommendations for Payment Service Providers

Based on analysis of the threats, vulnerabilities and consequences, as well as risk assessments concerning money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in non-bank payment service providers and non-bank money changers, the following recommendations apply to service providers:

1. Adopting the outcomes of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA) of the payment system to increase risk mitigation measures against money laundering, terrorist financing and proliferation financing as well as to strengthen implementation of a risk-based approach to anti-money laundering and combating the financing of terrorism (AML/CFT) in the operational activities.

2. Disseminating the outcomes of the National Risk Assessment (NRA) and Sectoral Risk Assessment (SRA) to all employees to raise awareness concerning the risks associated with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

3. Implementing public campaigns concerning the importance of anti-money laundering and combating the financing of terrorism (AML/CFT), while educating customers regarding the importance of implementing AML/CFT, particularly in terms of customer due diligence.

4. Strengthening implementation of a risk-based approach to anti-money laundering and combating the financing of terrorism (AML/CFT) through the application of regulatory technology (RegTech) in the identification and verification process, coupled with ongoing due diligence of the customer profiles and customer transactions.

BANK INDONESIA ACHIEVEMENTS

The prevention and eradication of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction (WMD) in Indonesia are not straightforward. The relevant government ministries/agencies have implemented a range of strategic policies, recapitulated as follows along with some of Bank Indonesia's salient achievements:

1. **Bank Indonesia has taken mitigation measures by promulgating the following regulations pertaining to non-bank payment service providers and non-bank money changers:**

    a. Bank Indonesia Regulation (PBI) No. 14/23/PBI/2012 concerning Money Transfers.

    b. Bank Indonesia Regulation (PBI) No. 18/20/PBI/2016 concerning Non-Bank Money Changers.

    c. Bank Indonesia Regulation (PBI) No. 19/10/PBI/2017 concerning the Application of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Non-Bank Payment Service Providers and Non-Bank Money Changers.

    d. Bank Indonesia Regulation (PBI) No. 20/2/PBI/2018, as an amendment to PBI No. 19/7/PBI/2017 concerning Carrying Foreign Banknotes Into and Out of the Territory of the Republic of Indonesia.

    e. Circular Letter No. 11/10/DKSP concerning Card-Based Payment Instrument Issuers.

    f. Circular Letter No. 15/23/DKSP concerning Non-Bank Money or Value Transfer Services (MVTS).

    g. Circular Letter No. 18/42/DKSP concerning Non-Bank Money Changers.

    h. Bank Indonesia Regulation (PBI) No. 22/23/PBI/2020 concerning the Payment System.

    i. Bank Indonesia Regulation (PBI) No. 23/6/PBI/2021 concerning Payment Service Providers (PJP).

    j. Bank Indonesia Regulation (PBI) No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PIP).

2. **Bank Indonesia has also published the following guidelines for non-bank payment service providers and non-bank money changers to prevent money laundering, terrorist financing and financing of proliferation of weapons of mass destruction:**

    a. Guidance for the Application of Risk-Based AML/CFT for Supervisors and Non-Bank Payment Service Providers as well as Non-Bank Money Changers.

    b. Risk-Based Tools for Supervisors and Non-Bank Payment Service Providers as well as Non-Bank Money Changers.

    c. Guidelines for Blocking and Freezing Funds Belonging to Individuals or Corporations Identified on the List of Suspected Terrorists and Terrorist Organisations (DTTOT).

    d. Guidelines for Blocking and Freezing Funds Belonging to Individuals or Corporations Identified on the Proliferation Financing List.

    e. Guidelines for Customer Due Diligence (CDD), including electronic CDD (e-CDD).

    f. Guidelines for Handling Unlicensed Non-Bank Money Changers.

    g. Supervisory Framework.

    h. Supervisory Guidelines for Non-Bank Payment Service Providers and Non-Bank Money Changers.

i. Guidelines for Monitoring Sanctions, including the Monitoring System.

j. Notice No. 20/271/DKSP/SRT/B, dated 24th May 2018, concerning the Prohibition of Recirculating the 10,000 Denomination Singaporean Dollar (SGD).

k. Notice No. 22/240/DKSP/SRT/B, concerning the Use of Digital Signatures and Payslips in the Issuance Process for Credit Cards.

l. Notice No. 22/221/DKSP/SRT/B, issued to non-bank payment service providers and non-bank money changers, concerning the Anticipation of Financial Crime during the Covid-19 Pandemic.

3. Bank Indonesia has attained the following achievements:

a. Risk and Policy

i. In 2019, Bank Indonesia formed the Anti-Money Laundering and Combating The Financing of Terrorism Division within the organisational structure. Bank Indonesia also established a multi-department AML/CFT Task Force in accordance with a Bank Indonesia Gubernatorial Decree.

ii. Applied a risk-based approach (RBA) to assessing risk profiles, oversight and inspections as well as implementation by service providers.

iii. Formulated and fully implemented the Annual Action Plan 2019-2021 of the National Anti-Money Laundering and Combating The Financing of Terrorism Strategy, with 100% accomplishment.

iv. Prohibited non-bank payment service providers and FinTech providers in Indonesia from processing payment transactions using virtual currency.

v. Bank Indonesia published the Indonesia Payment System Blueprint (BSPI) 2025, with AML/CFT commitment reflected in Vision 4, Safeguarding Balanced Innovation through Know Your Customer (KYC) Principles as well as Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT).

vi. As a member of the Money Laundering Committee, Bank Indonesia was actively involved in preparing the National Risk Assessment of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction in 2021.

vii. Bank Indonesia has promulgated several internal regulations relating to Anti-Money Laundering and Combating The Financing of Terrorism (AML/CFT) for service providers under the regulation and supervision of Bank Indonesia as follows:

a. Internal Board of Governors Regulation (PADG) No. 23/24/PADG INTERN/2021 concerning Guidance for Risk-Based Supervision of Anti-Money Laundering and Combating The Financing of Terrorism in Non-Bank Money Changers and Non-Bank Money or Value Transfer Services (MVTS).

b. Internal Board of Governors Regulation (PADG) No. 23/25/PADG INTERN/2021 concerning Guidance for Risk-Based Supervision of Anti-Money Laundering and Combating The Financing of Terrorism in Non-Bank Card-Based Payment Instrument Issuers as well as Non-Bank Electronic Money and Non-Bank Electronic Wallet Service Providers.

viii. Bank Indonesia published General Guidelines for Inspections under Specific Conditions as supervisory guidelines during the Covid-19 pandemic.

ix. The business process of carrying foreign banknotes constitutes an import-export activity into and out of the territory of the Republic of Indonesia, which can only be performed by a licensed business entity with a value equivalent to less than Rp1 billion. This regulation intends to prevent money laundering, acquire statistical data on carrying foreign banknotes and control counterfeit foreign banknotes, while strengthening information systems relating to cash.

x. Bank Indonesia prepared the Sectoral Risk Assessment (SRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021 as a follow-up to the National Risk Assessment (NRA) of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2021.

xi. Bank Indonesia compiled studies concerning AML/CFT implementation in non-bank money changers.

xii. Bank Indonesia compiled studies concerning current and emerging typologies of money laundering, terrorist financing and Financing of Proliferation of Weapons of Mass Destruction for non-bank payment service providers and non-bank money changers.

b. Licensing

i. Implementation of e-licensing for non-bank payment service providers and non-bank money changers, as well as carrying foreign banknotes since 2018.

ii. Application of the innovative QR Code in the logos of licensed non-bank money changers and non-bank Money or Value Transfer Services to help prospective customers identify and differentiate licensed and unlicensed service providers.

iii. Bank Indonesia has integrated the e-licensing system with the Indonesia National Single Window (INSW) to exchange information concerning the quota of licensed Cross-Border Cash Carriers (CBCC). Moving forward, the e-licensing system is expected to provide access to data and information on the identity of Cross-Border Cash Carriers (such as passport numbers and flight details) that can be accessed directly by the Directorate General of Customs and Excise (DJBC), Ministry of Finance, to assist the identification of Cross-Border Cash Carriers.

c. Supervision

i. Joint audits of non-bank payment service providers and non-bank money changers performed by the Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) and relevant government ministries/agencies.

ii. Bank Indonesia deploys the Bank Indonesia Surveillance and Supervision System (BI-SSS), which functions as an administrator of financial system data, while facilitating supervision analysis as well as the storage of assessment and inspection outcomes.

iii. Bank Indonesia conducts regular thematic supervision based on initiation by Bank Indonesia or input from other relevant authorities concerning emerging money laundering, terrorist financing and proliferation financing issues that demand attention.

iv. Imposition of sanctions and license revocation of non-bank payment service providers and non-bank money changers found in violation of Anti-

Money Laundering and combating the financing of terrorism (AML/CFT).

v. In 2021, non-bank money changers under the supervisory jurisdiction of Bank Indonesia underwent a relicensing process. Bank Indonesia issued relicensing policy requiring service providers to submit a license extension application every 5 years. The relicensing process takes into consideration the recommendations of supervisors and level of compliance to AML/CFT policy and regulations based on off-site and on-site supervision.

vi. In the licensing process, Bank Indonesia coordinates intensively with domestic authorities (Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), Corruption Eradication Commission (KPK), National Narcotics Agency (BNN), Indonesian National Police (POLRI), Financial Services Authority (OJK), Indonesia Deposit Insurance Corporation (IDIC), Ministry of Communication and Informatics as well as the Ministry of Trade), international organisations and other central banks to obtain additional information on prospective service providers.

vii. Bank Indonesia is currently developing Regulatory Technology (RegTech) and Supervisory Technology (SupTech) for subsequent implementation in the Bank Indonesia Supervision System.

d. Enforcement

i. Control of unlicensed non-bank money changers and illegal non-bank Money or Value Transfer Services in coordination with the Indonesian National Police and relevant government ministries and agencies. From 2017-2021, Bank Indonesia identified 1,090 unlicensed non-bank money changers and 79 illegal non-bank Money or Value Transfer Services in Indonesia. Bank Indonesia took immediate remediation measures through written warnings and other control measures in collaboration with the relevant authorities (Indonesian National Police).

ii. In 2017, the Bank Indonesia Representative Office in Bali cooperated with the Indonesian National Police to control the emergence of bitcoin ATMs.

iii. Bank Indonesia provided expert testimony on money transfers and currency exchange in criminal cases handled by the police, prosecution service and courts in Indonesia.

e. National Coordination

i. Bank Indonesia coordinates with the Directorate General of Customs and Excise (DJBC), Ministry of Finance, in relation to cross-border cash carriers via three integrated systems, namely Bank Indonesia e-licensing, Indonesia National Single Window (INSW) and Customs and Excise Information System and Automation (CESA).

ii. Bank Indonesia has signed memorandums of understanding (MoU) with government ministries/agencies concerning AML/CFT implementation, including MoUs with the Indonesian National Police (POLRI), Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), National Narcotics Agency (BNN), Corruption Eradication Commission (KPK) and Ministry of Finance. The scope of the MoUs include: (i) coordination and cooperation, (ii) supervision, (iii) task forces, (iv) information exchange, (v) socialisation activities, (vi) competency enhancement, (vii) taking action against unlicensed financial institutions.

iii. In conjunction with the Ministry of Finance, Bank Indonesia maintains a regular harmonisation forum that

convenes annually to discuss various aspects of joint concern, including cross-border cash carriers.

f. International Coordination

i. Memorandums of Understanding (MoU) between Bank Indonesia and other central banks have been expanded to include: (i) Bangko Sentral ng Pilipinas, (ii) Bank of Thailand (BoT), (iii) Bank Negara Malaysia, (iv) Brunei Darussalam Central Bank (BDCB), (v) Central Bank of the United Arab Emirates (CBUAE), and (vi) Monetary Authority of Singapore (MAS), in relation to AML/CFT implementation. The modality of the MoUs include: (i) policy dialogue, (ii) exchange of data and information, and (iii) capacity building.

ii. Bank Indonesia actively provides AML/CFT information based on requests from authorities in different jurisdictions, including the Australian Transaction Reports and Analysis Centre (AUSTRAC), Bank Negara Malaysia, Islamic Development Bank (IDB), Asia/Pacific Group on Money Laundering (APG) as well as members of the US Congress.

iii. Bank Indonesia was involved with the AML/CFT National Coordination Committee (NCC) in the context of preparing a Regional Risk Assessment (RRA) of Southeast Asia and Australia on Terrorist Financing 2017.

iv. Bank Indonesia was involved with the National Coordination Committee (NCC) in the context of preparing a Regional Risk Assessment (RRA) on Regional Threats to Transnational Money Laundering of Corruption Proceeds, involving ASEAN, Australia and New Zealand in 2019.

g. Communication and Outreach

i. Regular capacity building for Bank Indonesia supervisors throughout Indonesia as well as non-bank payment service providers and non-bank money changers through coordination meetings, workshops and coaching clinics.

ii. Bank Indonesia regularly standardises competencies in terms of the payment system and rupiah currency management (SP-PUR) through training/certification for service providers under the regulatory and supervisory jurisdiction of Bank Indonesia.

iii. As a vehicle of AML/CFT policy communication, Bank Indonesia launched a special AML/CFT menu on the official Bank Indonesia website in 2019.

iv. In preparation for the FATF Mutual Evaluation (ME) on-site visit, Bank Indonesia compiled AML/CFT media campaign material, including banners installed at all non-bank money changers and non-bank Money or Value Transfer Services under the regulatory and supervisory jurisdiction of Bank Indonesia as well as campaign content for television, newspapers and online media. In addition, Bank Indonesia cooperated with PT Ankasa Pura 2 to install AML/CFT communication media via digital banners at 19 airports in Indonesia.

Glossary of Terms and Abbreviations

Abbre-viation	Description
AinS	Account Information Services
AIS	Account Issuance Services
AKKI	The Indonesia Credit Card Association
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
APG	Asia/Pacific Group on Money Laundering
APH	Law Enforcement Agency/ies
APMK	Card-Based Payment Instruments
AUD	Australian Dollar
AUSTRAC	Australian Transaction Reports and Analysis Centre
BDCB	Brunei Darussalam Central Bank
BEC	Business Email Compromise
BI-SSS	Bank Indonesia Surveillance and Supervision System
BNM	Bank Negara Malaysia
BNN	National Narcotics Agency
BNPT	National Counter-Terrorism Agency
BOT	Bank of Thailand
BPR	BPR
BSP	Bangko Sentral Ng Pilipinas
BSPI	Indonesia Payment System Blueprint
CBCC	Cross-Border Cash Carriers
CBPI	Card-Based Payment Instrument
CBUAE	Central Bank of United Arab Emirates
CDD	Customer Due Diligence
CESA	Custom Excise Information System and Automation
CFATF	Caribbean Financial Action Task Force
CFT	Combating the Financing of Terrorism
CNY	Yuan
CTED	Counter-Terrorism Committee Executive Directorate
CTR	Cash Transaction Report
CV	Limited Partnership Company
DFS	Digital Financial Services
DHN	National Blacklist
DJBC	Directorate General of Customs and Excise
DTTOT	List of Suspected Terrorists and Terrorist Organisations
EDD	Enhanced Due Diligence
EIT	Electronic Information and Transactions
E-KYC	Electronic Know Your Customer
EUR	Euro
FATF	Financial Action Task Force on Money Laundering
FDS	Fraud Detection System
FGD	Focus Group Discussions
FPC	Foreign Predicate Crime
FTFs	Foreign Terrorist Fighters
GSP	Providers of Goods and/or Other Services

IDB	Islamic Development Bank
INSW	Indonesia National Single Windows
Interpol	International Criminal Police Organisation
INTRAC	Indonesian Financial Transaction Reports and Analysis Centre
IP	Internet Protocol
KPK	Corruption Eradication Commission
KUPVA	Non-Bank Money Changers
KYC	Know Your Customer
LO	Laundering Offshore
LPP	Supervisory and Regulatory Body
MAS	Monetary Authority of Singapore
MER	Mutual Evaluation Review
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and Terrorism Financing
MoU	Memorandum of Understanding
MSB	Money Service Businesses
MVTS	Money Or Value Transfer Services
MYR	Malaysian Ringgit
NCC	National Coordination Committee
NGO	Non-Governmental Organisations
NPL	Non-Performing Loans
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development
OJK	Financial Services Authority
PADG	Internal Board of Governors Regulation
PBI	Bank Indonesia Regulation
PEPs	Politically Exposed Persons
PFWMD	Financing of Proliferation of Weapons of Mass Destruction
PIAS	Payment Initiation and/or Acquiring Services
PIN	Personal Identification Number
PIP	Payment System Infrastructure Providers
PJP	Payment Service Providers
PMI	Indonesian Migrant Workers
PML	Professional Money Launderers
POLRI	Indonesian National Police
PPAT	Land Deed Officials
PPP	Public Private Partnership
PT	Limited Liability Company
QRIS	Quick Response Code Indonesia Standard
RBA	Risk-Based Approach
RegTech	Regulatory Technology
RRA	Regional Risk Assessment
SEBI	Bank Indonesia Circular Letter
SGD	Singaporean Dollar
SLIK	Financial Information Services System
SPI	Indonesia Payment System
SP-PUR	Payment System and Rupiah Currency Management
SRA	Sectoral Risk Assessment
STR	Suspicious Transaction Report
Stranas	National Strategy
SupTech	Supervisory Technology
TEKFIN	Financial Technology (FinTech)
THB	Thai Baht

TKT	Cash Transaction Reports
TF	Terrorist Financing
UKA	Foreign Banknote
UN	United Nations
USD	US Dollar
WFH	Work from Home

References

APG. 2021. APG Yearly Typologies Report: Methods and Trends of Money Laundering and Terrorist Financing. http://www.apgml.org/methods-and-trends/page.aspx?p=8d052c1c-b9b8-45e5-9380-29d5aa129f45

Bank Indonesia. 2016. Bank Indonesia Regulation No.18/20/PBI/2016 concerning Non-Bank Money Changers. https://www.bi.go.id/en/publikasi/peraturan/Documents/pbi_182016_EN.pdf

Bank Indonesia. 2017. Bank Indonesia Regulation No.19/10/PBI/2017 concerning the Implementation of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) for Payment System Service Providers and Non-Bank Money Changers. https://www.bi.go.id/en/publikasi/peraturan/Documents/pbi_191017.pdf

Bank Indonesia. 2019. Sectoral Risk Assessment of Money Laundering and Terrorist Financing in Payment System Service Providers and Non-Bank Money Changers. https://www.bi.go.id/en/fungsi-utama/sistem-pembayaran/anti-pencucian-uang-dan-pencegahan-pendanaan-terrorisme/Documents/SRA_en.pdf

Bank Indonesia. 2020. Bank Indonesia Regulation No. 22/23/PBI/2020 concerning the Payment System. https://www.bi.go.id/en/publikasi/peraturan/Documents/PBI_222320.pdf

Bank Indonesia. 2021. Bank Indonesia Regulation No. 23/6/PBI/2021 concerning Payment Service Providers. https://www.bi.go.id/en/publikasi/peraturan/Documents/PBI_230621_EN.pdf

Bank Indonesia. 2021. Bank Indonesia Regulation No. 23/7/PBI/2021 concerning Payment System Infrastructure Providers (PIP). https://www.bi.go.id/elicensing/helps/PBI_230721%20Penyelenggara%20Infrastruktur%20Sistem%20Pembayaran.pdf

BNPT, INTRAC, Special Detachment 88, POLRI, BIN. 2017. White Paper: Mapping Risk of Terrorist Financing in Relation to Terrorist Networks. Jakarta: BNPT.

Digital Market Outlook. 2020. Digital Transactions. https://www.statista.com/outlook/digital-markets

FATF. 2010. Report on Money Laundering Using New Payment Methods. https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

FATF. 2013. FATF Guidance on National Money Laundering and Terrorism Financing Risk Assessment. https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

FATF. 2013. Guidance for A Risk-Based Approach: Prepaid Cards, Mobile Payments And Internet-Based Payment Services. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

FATF. 2013. Guidance on Politically Exposed Persons. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

FATF. 2015. Emerging Terrorist Financing Risks. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

FATF. 2016. Guidance for A Risk-Based Approach Money Or Value Transfer Services. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

FATF. 2018. Professional Money Laundering. https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

FATF. 2019. Terrorist Financing Risk Assessment Guidance. https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf

FATF. 2020. Risk and Policy Responses on COVID-19 related Money Laundering and Terrorist Financing. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

FATF. 2021. International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF. 2021. Guidance on Proliferation Financing Risk Assessment And Mitigation. https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

INTERPOL. 2020. Preventing Crime and Protecting Police: INTERPOL's COVID-19 Global Threat Assessment. https://www.interpol.int/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

The United Nation Security Council Counter-Terrorism Committee Executive Directorate (CTED). 2021. The Impact of the COVID-19 Pandemic on Terrorism, Counter-Terrorism and Countering Violent Extremism. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jun/cted_covid_paper_15june2021_1.pdf

2021. Indonesia Risk Assessment of Money Laundering 2021.

2021. Indonesia Risk Assessment of Terrorist Financing and Financing the Proliferation of Weapons of Mass Destruction 2021.

Compilation Team

SECTORAL RISK ASSESSMENT OF MONEY LAUNDERING, TERRORIST FINANCING AND FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION IN NON-BANK PAYMENT SERVICE PROVIDERS AND NON-BANK MONEY CHANGERS (2021)

ADVISOR
Doni Primanto Joewono - Filianingsih Hendarta - Fitria Irmi Triswati

COORDINATOR AND EDITOR
Elyana K. Widyasari

DRAFTING TEAM
Feronika R. Sipayung - Nabila Femiliana - Hashina Nurul Nida

CONTRIBUTOR
Financial System Surveillance Department
Regional Department
Bank Indonesia Representative Offices

INSTITUTIONAL CONTRIBUTOR
Indonesian Financial Transaction Reports and Analysis Centre (INTRAC)
Mardiansyah - Vidyata Annisa Anafiah

FULL REPORT IS AVAILABLE FOR DOWNLOAD IN PDF FORMAT AT BANK INDONESIA WEBSITE:
https://www.bi.go.id

FOR INQUIRIES, COMMENT AND FEEDBACK PLEASE CONTACT:
Bank Indonesia
Payment System Policy Department
Jl. MH Thamrin No. 2, Jakarta, Indonesia
Email: DKSP-APUPPT@bi.go.id,
Phone: 131 (local), 1500131 (international)