2023

SECTORAL RISK

ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING IN FINANCIAL TECHNOLOGY

KPK
Komisi Pemberantasan Korupsi

BNN

KOMISI PEMILIHAN UMUM

KEMENTERIAN PERDAGANGAN
REPUBLIK INDONESIA

OJK
OTORITAS JASA KEUANGAN

BAWASLU

SECTORAL RISK
ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING IN FINANCIAL TECHNOLOGY
2023

Book Size	:	295 x 210 mm
Manuscript	:	Sectoral Risk Assessment of Money Laundering and Terrorist Financing in Financial Technology 2023
Published by	:	Indonesian Financial Transaction Reports and Analysis Center

FURTHER INFORMATION

Indonesian Financial Transaction Reports and Analysis Center (INTRAC)

Jl. Ir. H. Juanda No. 35 Jakarta 10120 Indonesia

Phone: (+6221) 3850455, 3853922

Fax: (+6221) 3856809 – 3856826

Website: http://www.ppatk.go.id

TEAM

A. Steering Committee

1. Chief of the Criminal Chamber, Supreme Court of the Republic of Indonesia
2. Head of the AML/CFT Group, Financial Services Authority
3. Deputy Attorney General for Special Crimes, Attorney General's Office of the Republic of Indonesia
4. Director of Terrorism and Transnational Crimes, Attorney General's Office of the Republic of Indonesia
5. Director of Special Economic Crimes, Criminal Investigation Agency, Indonesian National Police
6. Director of Investigation, Densus 88 Anti-Terror Police Unit
7. Director of Intelligence, Densus 88 Anti-Terror Police Unit
8. Director of Development of Inter-Commission and Inter-Agency Networks (PJKAKI), Corruption Eradication Commission
9. Director of Money Laundering Crimes, National Narcotics Agency
10. Director of Domestic Strategy and Cooperation, INTRACT
11. Director of Reporting, INTRACT
12. Director of Compliance Supervision for Financial Service Providers, INTRACT
13. Head of the Payment System Policy Department, Bank Indonesia
14. Head of the Bureau of Commodity Futures Trading Supervision, Warehouse Receipt System, and Commodity Auction Market, Commodity Futures Trading Supervisory Agency
15. Head of the Bureau of Law and Public Relations, General Elections Supervisory Agency
16. Head of the Bureau of Legal Advocacy and Dispute Resolution, General Elections Commission

B. Implementation Team

1. Representative of the Supreme Court
   1) R. Heru Wibowo Sukaten
   2) Dwi Sugiarto
2. Representative of the Deputy Attorney General for Special Crimes, Attorney General's Office of the Republic of Indonesia
   1) Riyono
   2) Daniel Kristanto Sitorus
3. Representative of the Directorate of Terrorism and Transnational Crimes, Attorney General's Office of the Republic of Indonesia
   1) Erwin Indraputra
   2) Juwita Kayana
4. Representative of the Directorate of Special Economic Crimes, Criminal Investigation Agency, Indonesian National Police
   a) Putra Daniel Ibrani Hutagalung
   b) Eko Nugroho
5. Representative of the Special Anti-Terror Detachment, Indonesian National Police

   1) Daniel
   2) Jay Kesuma
6. Representative of the Financial Services Authority (OJK)
   1) Rinto Teguh Santoso
   2) Nelson S. E. Siahaan
   3) Adriane W. Wiryawan
   4) Rifki Arif Budianto
   5) Arum Sulistiyaningsih
7. Representative of Bank Indonesia
   1) Danarto Tri Sasongko
   2) Tita Sylvia Rachma
8. Representative of the Commodity Futures Trading Supervisory Agency, Ministry of Trade
   1) Athika Budi Prihatini
   2) Theresia Wahyuni
9. Representative of the Corruption Eradication Commission
   1) Amarillys Enika N.A.
   2) M. K. Gumilang
10. Representative of the National Narcotics Agency
   1) Agus Darojat
   2) Galuh Wijayanto Adi Wibowo
11. Representative of the General Elections Supervisory Agency
   1) R. Alief Sudewo
   2) Kelfin Roy Dominikus Boseren
   3) Andi Syahbudin
   4) Geano Giovan Naldi
12. Representative of the General Elections Commission
   1) Yulie Fitria Setianti
   2) Tota Pasaribu
   3) Rahmat Sugianto
   4) Rizka
13. Internal INTRAC
   1) Rachmawati
   2) Aris Priatno
   3) Mohammad Shalehuddin Akbar
   4) Tri Puji Raharjo
   5) Mardiansyah
   6) Vidyata Annisa A.
   7) Sheilla Yudiana
   8) Kristina Widhi
   9) Riana Rizka
   10) Patrick Irawan
   11) Trinanda Ramadhan
   12) Ferti Srikandi Sumanthi
   13) Muh. Afdal Januar
   14) Merlinda Fenisa
   15) Rieke Widasari
   16) Hendra Pradana Yulianto
   17) Hanindya Candrasari
   18) Nadya Tri Oktary
   19) Andini Novita Sari
   20) Afrian Novia Kartikasari
   21) Ayudianti
   22) Novie Eriska Aritonang
   23) Tri Indah Purwanti
   24) M. Aries Setyawan
   25) Dian Adelia
   26) Tria Rizki Safitri
   27) Adhitya Abriansyah Afandi
   28) Aman Subanjar
   29) M. Natsir Kongah
   30) Faris Adi Dharmawan

EXECUTIVE SUMMARY

The history of financial technology worldwide can be said to have begun around 1886 when the first transatlantic cable was built, enabling cross-border transfers. In Indonesia, fintech may be considered to have started with the introduction of ATM machines in 1987 by Bank Niaga, followed by e-banking services introduced by Bank Internasional Indonesia in 1988. In 2015, digital online payment systems became available in Indonesia, and in the same year the Indonesian Fintech Association and the Indonesian Joint Funding Fintech Association were established. In 2016 and the years that followed, along with the growing use of the internet and social media in Indonesia, innovations in financial services emerged, marked by the establishment of fintech companies in the country.

There are numerous types of fintech in Indonesia; however, for the purposes of this SRA (Sectoral Risk Assessment report), we limit the discussion to four categories: payments (including fund transfers—payments and remittances), lending, crowdfunding, and investment. The supervision and regulation of fintech in Indonesia are carried out by regulatory and supervisory authorities, including Bank Indonesia (BI), the Financial Services Authority (OJK), and the Commodity Futures Trading Supervisory Agency (Bappebti). The roles of supervisory and regulatory agencies in mitigating money laundering (ML) and terrorist financing (TF) risks in fintech include issuing regulations, supervision and sanctions, designating official service-provider associations, conducting outreach to both service providers and the public, as well as cooperation and coordination with domestic ministries/agencies and competent foreign authorities.

The scope of the 2023 Fintech SRA includes identifying the types of fintech operating in Indonesia; identifying and analyzing ML and TF risks across fintech types—which consist of ML threats, ML and TF typologies, geographical/provincial distribution and perpetrator profiles—as well as identifying potential risks of fintech misuse in general elections. The guidelines used in preparing the 2023 Fintech SRA refer to international best practices, including the National Money Laundering and Terrorist Financing Assessment (FATF Guidance), Risk Assessment Support for Money Laundering/Terrorist Financing (World Bank), Review of the Fund’s Strategy on Anti–Money Laundering and Terrorist Financing (IMF), and the Terrorist Financing Risk Assessment Guidance.

Using data from 2019 to June 2023, sourced from statistics on suspicious transaction reports, supervisory activities, FIU information exchange, financial intelligence reports, investigations, prosecutions and court decisions, as well as self-assessments by experts representing reporting parties, supervisory and regulatory authorities, the FIU/financial intelligence units (INTRAC), and law enforcement apparatus—an ML/TF risk assessment of fintech was conducted. Qualitative data collection was carried out through questionnaires submitted to supervisory and regulatory authorities, law enforcement apparatus, relevant ministries/agencies, and reporting parties, with a total of 20 respondents and an average response rate of 95%. In addition to the questionnaire, data collection also included interviews with 3 representatives of supervisory and regulatory authorities, 4 representatives of law enforcement apparatus, and 11 representatives of reporting parties to obtain deeper insights into ML and TF risks in fintech.

The key findings of the 2023 ML/TF SRA on fintech are as follows:

1. In general, ML and TF perpetrators have not extensively used fintech, and still rely more heavily on “conventional” financial institutions and designated non-financial businesses and professions (DNFBP). This is based on respondents’ perceptions and field findings indicating that there have not been many ML/TF cases involving fintech.
2. Fintech reporting parties are considered to have fairly strong risk-mitigation capabilities. Fintech entities are viewed as having implemented modern technological tools that facilitate monitoring and supervision, and they generally employ personnel with strong competencies, many of whom come from conventional industries.
3. Supervision and regulation of fintech by supervisory/regulatory agencies are considered adequate. Supervisory/regulatory agencies have issued sufficient regulations and conducted outreach to reporting parties under their supervision.
4. Law enforcement apparatus declare that their capability to handle fintech-related matters is fairly good, as indicated by training and education on fintech, as well as broad cooperation frameworks for handling cases.
5. The main ML and TF risks in fintech include:

Points of Concern/PoC	**ML**	**TF**
Types of Fintech	1. Investment 2. Remittance and payment	Lending
ML Predicate Offense	Fraud	[redacted]
Typologies	1. Asset purchases (property, vehicles, crypto assets, etc.) 2. Structuring (breaking transactions into smaller amounts but conducted multiple times by one person) 3. Smurfing (breaking transactions into smaller amounts conducted by several individuals)	1. Use of funds – domestic terrorism operations – false identity documents 2. Fund collection – legal
Regions	DKI Jakarta	1. West Java 2. DKI Jakarta
Profiles	Entrepreneurs business owners	

6. Most respondents (67%) believe that there is potential misuse of fintech in general elections, with examples of identified risks including:
   a. The use of crypto assets to hold election funds or receive campaign donations.
   b. The use of digital wallets or electronic money for “serangan fajar” (vote-buying operations) and for structuring/breaking up transactions.

c. Online lending used for the collection of funds.
d. Repayment of online loans belonging to election candidates by third parties.
e. Collusion between lenders and borrowers in online lending. In online lending or peer-to-peer lending, lenders must approve the loans that will be granted to borrowers. Generally, lenders and borrowers in LPBBTI (Information Technology–Based Joint Funding Services) do not know each other, but in this case the lender and borrower are acquainted, allowing collusion to occur.

7. There were one (1) ML case study, two (2) TF case studies, and one (1) predicate offense case study identified involving fintech over the past five years in Indonesia.

Furthermore, stakeholders identified several additional developments that may potentially be used more extensively in the future, based on observations of suspicious financial transactions and recent ML and TF case handling trends, including:

a. Payments and Remittances
   i. Transactions using complex layering schemes, for example: deposit and withdrawal transactions that do not directly use bank accounts but pass through several transaction services (such as digital wallets or currency-conversion websites);
   ii. Misuse of electronic wallets for storing and transferring proceeds of online gambling;
   iii. Cash-withdrawal and cash-deposit features used as mechanisms to obscure the flow of funds; and
   iv. Cross-border QRIS payments.

b. Lending
   i. Collusion between funders and borrowers in LPBBTI; and
   ii. Virtual-account payments for LPBBTI transactions that do not use the bank account registered to the LPBBTI user account.

c. Crowdfunding

For crowdfunding activities, we did not obtain examples of new ML or TF threats from respondents; however, in the context of elections we identified the potential for campaign-fund collection through social crowdfunding mechanisms. Crowdfunding itself is not inherently illegal, but it can obscure the origin of funds because the sources come from the public, and it may also potentially exceed the legal donation limits for individuals.

d. Investment
   i. Off-market crypto transactions (transactions on private blockchains, direct individual-to-individual or Person-to-Person/P2P transactions);
   ii. Crypto-asset transactions conducted using foreign exchangers;
   iii. Investments through e-commerce, such as online mutual-fund investments or gold-investment services that collaborate with e-commerce platforms;
   iv. Digital-wallet/e-money transaction agreements conducted through social media (usually for the purchase and sale of crypto assets);
   v. Non-Fungible Tokens (NFTs); and
   vi. Investment payments made by third parties.

e. Others
   i. Creation of fictitious corporate (merchant) accounts used for money-laundering activities; and
   ii. Misuse of Buy Now, Pay Later (BNPL) facilities by criminals to purchase goods.

FOREWORD

Financial technology, or fintech, has emerged alongside changes in societal lifestyles that demand speed and convenience. Fintech enables the public to conduct remote transactions within seconds. While these technological developments support daily life, they may also be misused by criminals to commit money laundering (ML) and terrorist financing (TF) crimes.

In 2017, the FATF (Financial Action Task Force)—as the international body responsible for anti–money laundering and counter-terrorist financing (AML/CTF)—stated that it “strongly supports responsible financial-technology innovation that is in line with the AML/CFT requirements contained in the FATF Standards, and will continue to explore opportunities presented by fintech and regulatory developments to strengthen the effective implementation of AML/CFT measures.” Indonesia, as a member of the FATF, naturally supports this view.

The Government of Indonesia has demonstrated significant and progressive steps, together with all relevant stakeholders, in supporting fintech innovation while simultaneously strengthening and consolidating supervisory and regulatory efforts at the national level—both through the National Coordination on the Prevention and Eradication of Money Laundering and Terrorist Financing (the ML Committee) and the Investment Alert Task Force (SWI). The Government also monitors ML and TF risks in Indonesia’s developing fintech landscape through the preparation of the 2023 Sectoral Risk Assessment Report on Money Laundering and Terrorist Financing in Fintech.

Therefore, I warmly welcome the preparation of the 2023 Sectoral Risk Assessment of Money Laundering and Terrorist Financing in Financial Technology, and I hope it will be promptly followed by strategic actions and mitigation measures to address the risk developments identified by all relevant stakeholders. Finally, I extend my appreciation and gratitude to everyone who contributed to the preparation of this Sectoral Risk Assessment Report of Money Laundering and Terrorist Financing in Financial Technology 2023.

Jakarta, January 2024
Signed
Dr. Ivan Yustiavandana, S.H., LL.M.
Head of the Financial Transaction Reports and Analysis Center

LIST OF ABBREVIATIONS AND TERMS

NO.	Abbreviation/Term	Definition
1	AMLC	Anti-Money Laundering Council (Philippines FIU)
2	AMLO	Anti-Money Laundering Office (Thailand FIU)
3	APH	Law Enforcement Agency
4	AML–CFT	Anti–Money Laundering and Countering the Financing of Terrorism
5	Bappebti	Commodity Futures Trading Regulatory Agency
6	BI	Bank Indonesia
7	CPFAX	Prospective Physical Crypto Asset Trader
8	DNFBP	Designated Non-Financial Businesses and Professions
9	DPPSPM	List of Weapons of Mass Destruction Proliferation Financing
10	DTTOT	List of Suspected Terrorists and Terrorist Organizations
11	FATF	Financial Action Task Force
12	FMU	Financial Monitoring Unit (Pakistan NTRAC)
13	FSA	Financial Services Authority (OJK)
14	FSI	Financial Service Institutions (LJK)
15	LPBBTI	Information Technology–Based Joint Funding Services
16	LUDBTI	Information Technology–Based Crowdfunding Services
17	MLA	Mutual Legal Assistance
18	MSB	Money Service Business
19	PSP	Payment Service Provider
20	INTRAC	Indonesian Financial Transaction Reports and Analysis Center (PPATK)
21	PPSPM	Weapons of Mass Destruction Proliferation Financing
22	SECP	Securities and Exchange Commission Pakistan
23	SRA	Supervisory and Regulatory Authority
24	Fintech	Financial Technology
25	PO	Predicate Offense
26	TF	Terrorist Financing
27	ML	Money Laundering
28	VASP	Virtual Asset Service Provider

TABLE OF CONTENTS

TEAM 3

EXECUTIVE SUMMARY 5

FOREWORD 9

LIST OF ABBREVIATIONS AND TERMS 10

CHAPTER I — INTRODUCTION 16

1.1. Background 16

1.2. Objective 17

1.3. Output 18

CHAPTER II — FINANCIAL TECHNOLOGY 19

2.1. Financial Technology in Indonesia 19

a. History and Development of Financial Technology 19

b. History and Development of Financial Technology in Indonesia 20

c. Types of Financial Technology in Indonesia 20

2.2. Map of the Financial Technology Industry in Indonesia 24

a. Payments (including Remittance) 24

b. Lending 25

c. Crowdfunding 26

d. Investment 29

2.3. Supervision and Regulation of Financial Technology in Indonesia 30

a. Regulations for Financial Technology Providers 30

b. The Role of Supervisory and Regulatory Authorities in Risk Mitigation 31

2.4. FATF Recommendations Related to Financial Technology 32

CHAPTER III — RESEARCH METHODOLOGY 33

3.1. RESEARCH METHOD 33

3.2 SCOPE AND STEPS OF RISK ASSESSMENT 33

3.3. STAGES OF RISK ASSESSMENT 34

CHAPTER IV — RISK ASSESSMENT RESULTS 37

4.1. INTERVIEW FINDINGS 37

a. Threats, Vulnerabilities, and Impacts of Financial Technology According to Supervisory and Regulatory Authorities and “Conventional” DNFBPs 37

b. Capacity to Mitigate ML and TF Risks in Fintech 39

4.2. RISK ASSESSMENT 41

a. Types of Fintech 41

b. Predicate Offense for Money Laundering 42

c. ML Typologies 48

d. TF Typologies 52

e. Regions 59

f. Profiles 70

4.3. POTENTIAL RISKS OF FINTECH MISUSE IN GENERAL ELECTIONS 80

4.4. EMERGING THREATS 81

4.5. TYPOLOGIES AND CASE STUDIES 82

CHAPTER V — CONCLUSIONS AND RISK-MITIGATION STRATEGIES 90

5.1. CONCLUSIONS 90

5.2. RISK-MITIGATION STRATEGIES 92

BIBLIOGRAPHY 96

APPENDICES 98

LIST OF TABLES

Table 1 Peer-to-Peer Lending Fintech Statistics 26

Table 2 Number of Financial Technology Providers in Indonesia 29

Table 3 FSA Regulations for Financial Technology Providers 30

Table 4 Bank Indonesia Regulations for Financial Technology Providers 30

Table 5 Bappebti Regulations for Financial Technology Providers 31

Table 6 SRA Questionnaire and Interview Topics 36

Table 7 ML Risk by Type of Fintech 42

Table 8 TF Risk by Type of Fintech 42

Table 9 Predicate Offense with High ML Risk Related to Fintech 43

Table 10 Predicate Offense with High ML Risk Related to Payment Fintech and Remittance 44

Table 11 Predicate Offense with High ML Risk Related to Lending Fintech 45

Table 12 Predicate Offense with High ML Risk Related to Crowdfunding Fintech 46

Table 13 Predicate Offense with High ML Risk Related to Investment Fintech 47

Table 14 ML Typologies with High Risk in Fintech 48

Table 15 ML Typologies with High Risk in Payment and Remittance Fintech 49

Table 16 ML Typologies with High Risk in Lending Fintech 50

Table 17 ML Typologies with High Risk in Crowdfunding Fintech 51

Table 18 ML Typologies with High Risk in Investment Fintech 52

Table 19 TF Typologies with High Risk in Fintech 53

Table 20 TF Typologies with High Risk in Payment and Remittance Fintech 53

Table 21 TF Typologies with High Risk in Lending Fintech 55

Table 22 TF Typologies with High Risk in Crowdfunding Fintech 56

Table 23 TF Typologies with High Risk in Investment Fintech 58

Table 24 Regions with High ML Risk in Fintech 60

Table 25 Regions with High TF Risk in Fintech 61

Table 26 Regions with High ML Risk in Payment and Remittance Fintech 62

Table 27 Regions with High TF Risk in Payment and Remittance Fintech 63

Table 28 Regions with High ML Risk in Lending Fintech 64

Table 29 Regions with High TF Risk in Lending Fintech 65

Table 30 Regions with High ML Risk in Crowdfunding Fintech 66
Table 31 Regions with High TF Risk in Crowdfunding Fintech 67
Table 32 Regions with High ML Risk in Investment Fintech 68
Table 33 Regions with High TF Risk in Investment Fintech 69
Table 34 Profiles with High ML Risk in Fintech 70
Table 35 Profiles with High TF Risk in Fintech 71
Table 36 Profiles with High ML Risk in Payment and Remittance Fintech 72
Table 37 Profiles with High TF Risk in Payment and Remittance Fintech 73
Table 38 Profiles with High ML Risk in Lending Fintech 74
Table 39 Profiles with High TF Risk in Lending Fintech 75
Table 40 Profiles with High ML Risk in Crowdfunding Fintech 76
Table 41 Profiles with High TF Risk in Crowdfunding Fintech 77
Table 42 Profiles with High ML Risk in Investment Fintech 78
Table 43 Profiles with High TF Risk in Investment Fintech 79

LIST OF FIGURES

Figure 1	How Electronic Money/Digital Wallets Work	21
Figure 2	How Payment Gateway Works	21
Figure 3	How Peer-to-Peer Lending Works	22
Figure 4	How Multi-Asset Investment Applications Work	22
Figure 5	How Crowdfunding Works	23
Figure 6	Types of Digital Financial Innovation	24
Figure 7	Number of Licensed Electronic Payment Service Providers Based on Licensing Categories	25
Figure 8	Funds Raised Through LUDBTI, 2018–June 2022	28
Figure 9	Risk Assessment Formulation	33
Figure 10	Respondents' Perception of the Likelihood of Fintech Being Used by ML/TF Perpetrators Compared with "Conventional" Financial Institutions and DNFBPs	37
Figure 11	Respondents' Perception of Supervision and Regulation Related to AML/CFT in Fintech Compared with "Conventional" Financial Institutions and DNFBPs	38
Figure 12	Respondents' Perception of the Impact if ML/TF Occurs in Fintech Compared with "Conventional" Financial Institutions and DNFBPs	39
Figure 13	Respondents' Perception of the Potential for Fintech Misuse in General Elections	80
Figure 14	Example of ML Typology	83
Figure 15	Case Illustration: Indra Kusuma a.k.a. Indra Kenz	85
Figure 16	Case Study: Online Loan Misuse	86
Figure 17	Case Study: Online Loan Usage	87
Figure 18	Case Study: Salman Case	89
Figure 19	Case Illustration: Case 14	105

CHAPTER I INTRODUCTION

1.1. BACKGROUND

Developments in information technology and the increasing demands of a fast-paced lifestyle have led to changes in societal behavior. These technological developments greatly assist the public in meeting their needs, including access to financial services. However, on the other hand, such technological advancements also carry potential risks which, if not appropriately mitigated, may disrupt the integrity of the financial system.

One form of these technological developments is financial technology, or fintech, also referred to as Digital Financial Innovation (DFI). Fintech or DFI is defined as follows:

1. Financial technology is the use of technology in the financial system that generates new products, services, technologies, and/or business models, and that may affect monetary stability, financial-system stability, and/or the efficiency, smoothness, security, and reliability of the payment system (Bank Indonesia, 2017).
2. Digital Financial Innovation (DFI) refers to the renewal of business processes, business models, and financial instruments that provide new added value in the financial-services sector by involving the digital ecosystem (Financial Services Authority, 2018).

Although fintech has recently become increasingly popular, its history can be traced back to 1866, marked by the establishment of the first transatlantic cable linking America and Europe, and later the introduction of the first ATM system by Barclays in 1967. During this period, the financial sector had already adopted technologies such as the telegraph, which facilitated cross-border financial connectivity by enabling the rapid transmission of financial information, transactions, and payments worldwide. According to the Financial Services Authority, the main types of fintech in Indonesia include:

1. Payment startups;
2. Lending. This includes peer-to-peer lending or information-technology-based lending services (a platform that brings together borrowers and lenders), or functioning solely as a borrowing service;
3. Financial planning or personal finance;
4. Retail investment;
5. Financing or crowdfunding. Fundraising activities may be conducted for social or commercial purposes. For commercial purposes, one type of fintech regulated in Indonesia is equity crowdfunding or Information-Technology-Based Stock-Offering Fundraising Services, which have since evolved into securities crowdfunding;
6. Remittances (fund transfers); and
7. Financial research. This typically takes the form of aggregators or websites or applications that help the public/consumers obtain information on financial-service products and services by collecting, filtering, and comparing products and services across Financial Service Institutions (FSI) digitally.

FATF Recommendation 15 states that financial institutions must pay special attention to the risks of money laundering that may arise from new or developing technologies that support anonymity and take necessary measures to prevent their use for money laundering when required. In 2016 and 2019, Indonesian Financial Transaction Reports and Analysis Center (INTRACT) conducted research on crypto assets as part of the fintech domain. Then in 2019, INTRACT identified the threat of election-campaign funds being channeled through donation-based crowdfunding mechanisms. In 2021, Indonesia's National Risk Assessment (NRA) concluded that the use of illegal or unlicensed peer-to-peer lending constituted an emerging threat for money laundering and terrorist financing in Indonesia.

To mitigate the risks that may arise from the use of fintech in money laundering and terrorist financing, one of the actions taken is the development of a sectoral risk assessment. A sectoral assessment is expected to provide better understanding of the various factors within fintech, allowing identification of the highest-risk areas and enabling effective and efficient mitigation. Therefore, a Sectoral Risk Assessment (SRA) of Money Laundering (ML) and Terrorist Financing (TF) in fintech is necessary.

In addition, in anticipation of the 2024 political year, during which presidential, vice-presidential, legislative, and regional elections will be held, this assessment is also expected to help mitigate potential risks of misuse of campaign-funding regulations that may involve fintech.

1.2. OBJECTIVE

The SRA study of ML and TF in fintech is intended to identify, analyze, evaluate, and mitigate ML and TF risks present in fintech, with the specific objectives to:

1. Identify the types of fintech operating in Indonesia;
2. Identify and analyze ML risks in the various types of fintech in Indonesia based on predicate offenses for money laundering, regions or provinces, perpetrator profiles for ML and TF, and ML/TF typologies;
3. Identify potential risks of fintech misuse for election campaign financing;
4. Obtain case-study insights and identify suspicious-transaction indicators for fintech; and
5. Identify good practices in mitigating ML and TF risks in fintech.

1.3. OUTPUT

In general, this sectoral risk assessment on money laundering and terrorist financing in financial technology helps enhance understanding of the risks and challenges in addressing ML and TF offenses involving fintech, providing several benefits, including:

a. Building Awareness, Outreach, and Risk-Based Supervision

   The results of the ML and TF SRA on fintech will help raise awareness and outreach among the public and fintech entities, as well as support the implementation of risk-based supervisory policies.

b. Developing Scenarios for Detecting Suspicious Financial Transactions

   The results of the ML and TF SRA on fintech aim to assist in identifying specific risks related to the fintech sector and support the establishment of appropriate risk-mitigation measures. One mitigation step that reporting parties may take in utilizing the SRA results is to follow up by developing red-flag indicators or parameters of financial transactions that indicate suspected ML or TF, to accelerate detection and reporting to INTRAC.

c. Determining Priority Actions for Preventing and Combating ML and TF in Fintech

   By gaining a better understanding of the risks, the results of this ML and TF SRA on fintech can help determine priority actions needed in the fintech sector to mitigate risks. The findings of this SRA will also greatly assist law enforcement apparatus in conducting investigations and inquiries related to money laundering and terrorist financing offenses.

CHAPTER II FINANCIAL TECHNOLOGY

2.1. FINANCIAL TECHNOLOGY IN INDONESIA

a. History and Development of Financial Technology

Financial technology, often referred to as fintech (financial technology), is a combination of the words "technology'' and "financial," meaning innovation in financial services. According to Bank Indonesia, the combination of financial services and technology transforms conventional business models into more modern ones. Transactions that previously required face-to-face interaction and the physical exchange of cash can now be conducted remotely, with payments completed in just seconds.[1] Meanwhile, according to the Financial Services Authority (FSA), "Fintech is an innovation in the financial services industry that utilizes technological advancements. Fintech products generally consist of systems designed to execute specific financial-transaction mechanisms."[2]

The history of fintech can be divided into three periods, including fintech 1.0 (1886–1967), fintech 2.0 (1967–2008), and fintech 3.0 (2008–present). The first stage began with the development of the transatlantic cable in 1866, which enabled cross-border fund transfers. Then in 1967, Barclays introduced the first ATM, marking the beginning of fintech 2.0. In 1970, NASDAQ, the world's first digital stock exchange, was established. In the same year, SWIFT (Society for Worldwide Interbank Financial Telecommunications) was created as a communication protocol among financial institutions that facilitates large-scale cross-border payments. The introduction of the World Wide Web (WWW) internet banking protocol by Wells Fargo in 1995 gave customers their first internet-banking experience, followed by the emergence of branchless banking services such as ING Direct and HSBC Direct. PayPal was founded in 1998, enabling consumers worldwide to make payments and purchases. Following the 1997 Asian financial crisis, various financial and major technology companies began to adopt financial-services trends. The Global Financial Crisis (GFC) of 2008 is considered a major catalyst for the development of fintech 3.0, marked by declining public trust in established financial institutions, stricter regulations, and deteriorating political-economic conditions—all of which created opportunities for fintech startups to fill the gaps left by traditional financial services. This era also saw the emergence of Bitcoin (2009), which was predicted by some to replace global currency systems.

[1] Bank Indonesia. 1 December 2018. *"Understanding Financial Technology."* https://www.bi.go.id/id/edukasi/Pages/mengenal-Financial-Teknologi.aspx

[2] Financial Services Authority. *"FAQ Fintech Lending."* https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/direktori/fintech/Documents/FAQ%20Fintech%20Lending.pdf

b. **History and Development of Financial Technology in Indonesia**

Fintech can be considered to have "emerged" in Indonesia with the introduction of ATM machines by Bank Niaga in 1987, followed by BCA (Bank Central Asia) in 1998 and other banks thereafter.[3] In 1988, Bank Internasional Indonesia introduced Indonesia's first e-banking service. In its development, the most widely recognized service is KlikBCA, launched in 2001 due to its extensive use. In 2015, digital online payment systems became available in Indonesia. In the same year, the Indonesian Fintech Association and the Indonesian Joint Funding Fintech Association were established. Starting in 2016 and the years that followed, fintech companies began to emerge across Indonesia. The rapid growth of internet usage and social media contributed significantly to the rise of financial-service innovations in the country.

c. Types of Financial Technology in Indonesia

Types of fintech in Indonesia include:

1. **Payments**. These may take the form of electronic money (a payment instrument stored electronically in a specific medium such as a mobile application),[4] electronic wallets (electronic services for storing payment-instrument data using cards and/or electronic money, which may also hold funds for payment purposes), or payment gateways (electronic services that enable merchants to process payment transactions using instruments such as cards, electronic money, and/or bank payment services).

[3] Indonesian Joint Funding Fintech Association (Asosiasi Fintech Pendanaan Bersama Indonesia). *"History of Fintech Development in Indonesia."* https://afpi.or.id/articles/detail/sejarah-perkembangan-fintech-di-indonesia

[4] Electronic money also includes electronic money in the form of chip-based cards (electronic money cards); however, for the purposes of this SRA, only server-based electronic money will be discussed.

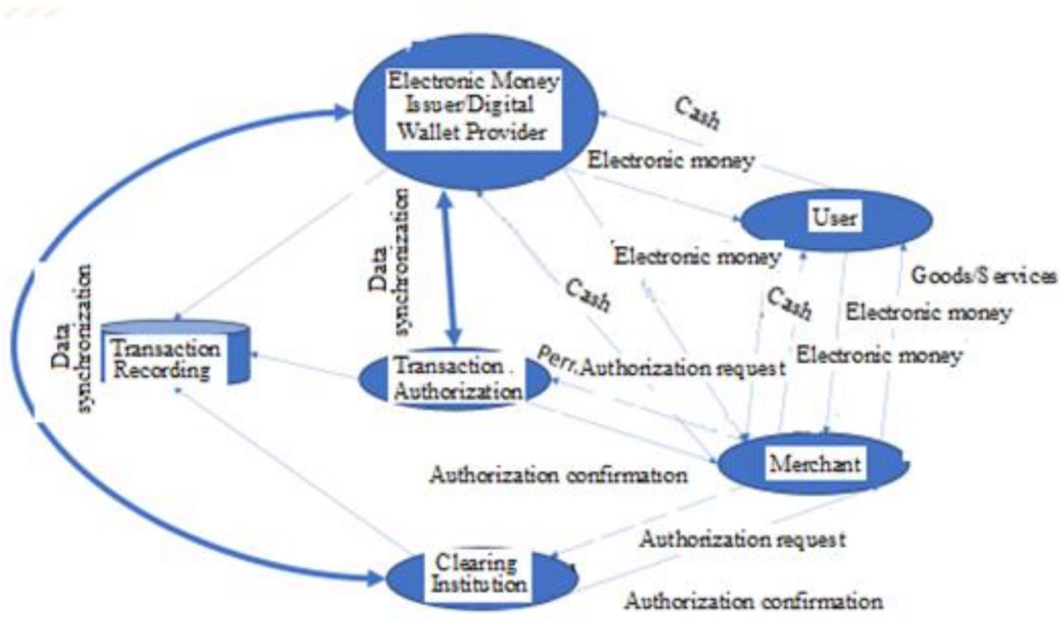


Figure 1. How Electronic Money/Digital Wallets Work

Source: Rahman (2013)

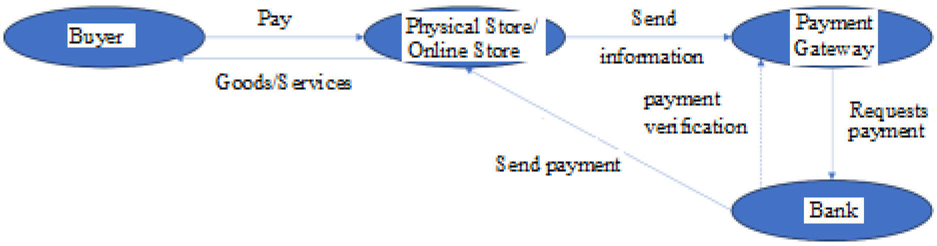
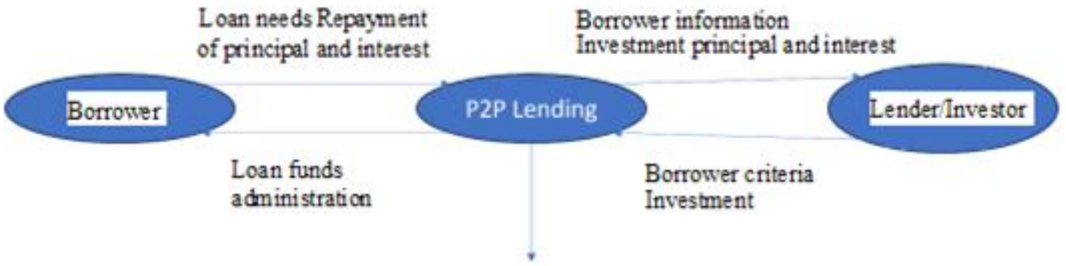


Figure 2. How Payment Gateway Works

Source: https://www.xendit.co/id/blog/cara-kerja-payment-gateway-dan-penerapannyadalam-bisnis-e-commerce-anda/

2. Lending. Lending may take the form of peer-to-peer lending or information-technology–based lending services (a platform that serves both borrowers and funders), or it may operate solely as a borrowing service.


Loan needs Repayment of principal and interest
Borrower information
Investment principal and interest
Borrower
P2P Lending
Lender/Investor
Loan funds administration
Borrower criteria
Investment

Analyzing data
– assessing risk
– drafting rules in accordance with Government regulations
– operations and administration
– technology and education
– balancing loan demand with the supply of funds from investors

Figure 3. How Peer-to-Peer Lending Works

Source: https://www.finansialku.com/ini-lho-cara-kerja-p2p-lending-konvensional-dan-p2p-lending-syariah/

3. **Retail investment**. Unlike traditional forms of investment, retail-investment fintech does not require users to first have a bank account. Investment placement can also be made in much smaller amounts than conventional investment products (starting from IDR 5,000).

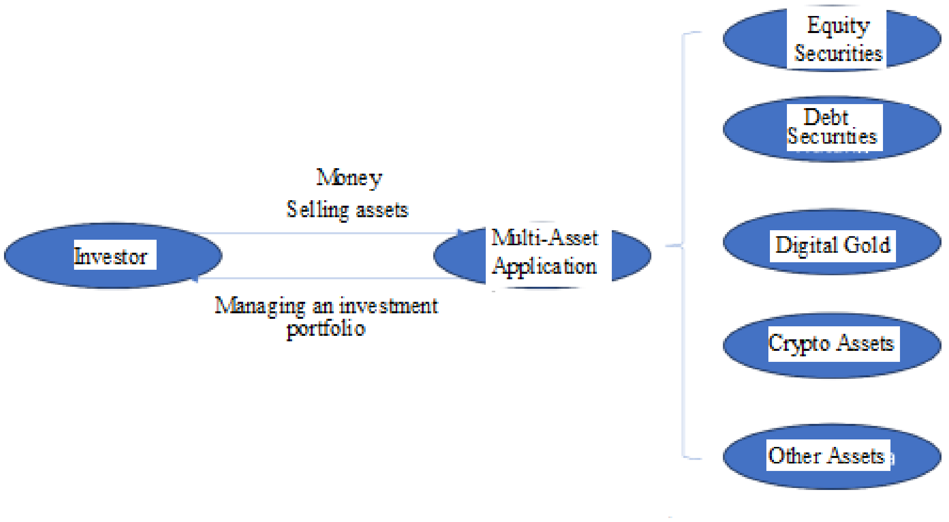


Figure 4. How Multi-Asset Investment Applications Work

4. **Financing or crowdfunding**. Fundraising may be conducted for social or commercial purposes. For commercial purposes, one type of fintech regulated in Indonesia is equity crowdfunding, or Information-Technology–Based Stock-Offering Fundraising Services, which has evolved into securities crowdfunding.

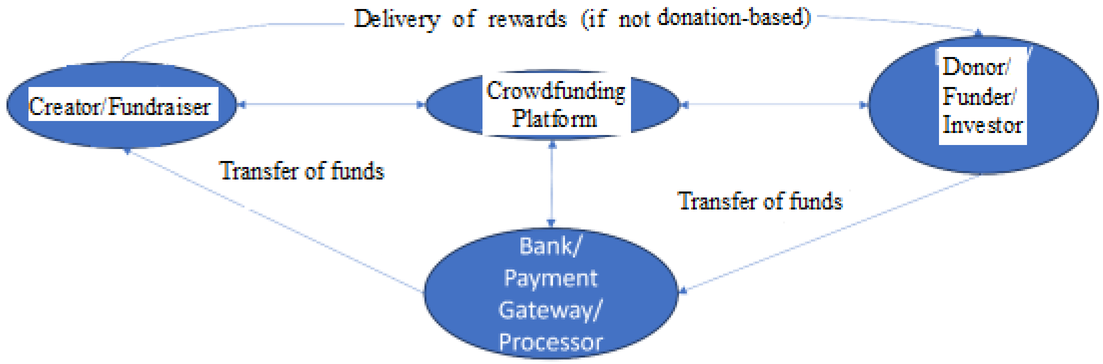


Figure 5. How Crowdfunding Works
Source

5. **Remittances (fund transfers)**.

In addition to the categories above, there are in fact many other types of fintech, although not all of them are directly related to financial transactions. Many fintech entities operate in areas that support financial services—for example, electronic know-your-customer (e-KYC) service providers, tax and accounting, insurtech (insurance technology), credit scoring, and others. According to FSA, fintech that is not directly related to financial transactions is classified as Digital Financial Innovation (DFI). As of the end of October 2023, there were 99 registered DFI providers categorized into 14 business-model clusters.

Figure 6. Types of Digital Financial Innovation

Source: FSA

2.2. THE LANDSCAPE OF THE FINANCIAL TECHNOLOGY INDUSTRY IN INDONESIA

Based on the scope of this SRA, the fintech sectors discussed in this report are limited to those directly related to financial transactions. For this SRA, we define four fintech categories (payments and remittances are grouped into a single cluster).

a. Payments, including Remittances

Bank Indonesia is the regulator for Payment Service Providers (PSP), which covers payment and fund-transfer services. Based on data obtained from Bank Indonesia, there are 258 licensed providers in the payment-system sector. Licenses for PSPs to conduct activities as specified in the regulations on Payment Systems and PSP provisions are granted based on licensing categories, which consist of:

1. Category I License, covering the following activities:
    a. Source-of-Funds Administration;
    b. Provision of Source-of-Funds Information;
    c. Payment initiation and/or acquiring services; and
    d. Remittance services.
2. Category II License, covering the following activities:
    a. Provision of Source-of-Funds Information; and
    b. Payment initiation and/or acquiring services.
3. Category III License, covering the following activities:
    a. Remittance services; and/or
    b. Other activities determined by Bank Indonesia.

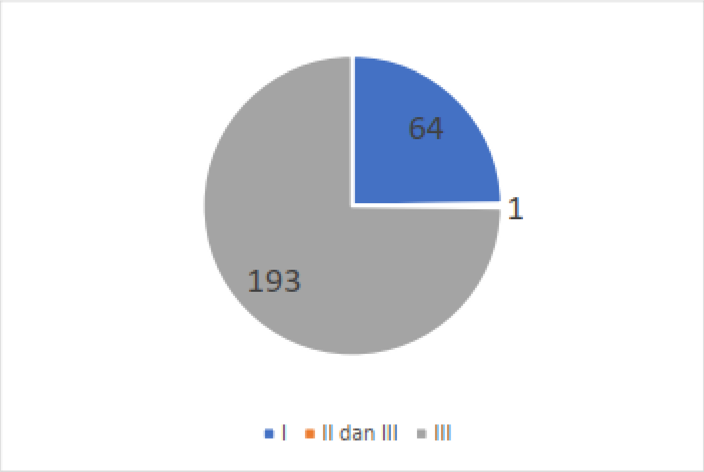


Figure 7. Number of Bank Indonesia–Licensed Payment Service Providers by Licensing Category
Source: Processed data

Of the 258 PSP providers, 102 providers offer Digital Financial Services (DFS). DFS refers to payment-system and financial-services activities carried out by PSPs that administer source-of-funds activities through the issuance of electronic money in cooperation with third parties, using mobile-based or other digital devices for digital economy purposes and inclusive finance.

According to Bank Indonesia data, prior to the pandemic, digital-wallet usage accounted for only around 10% of total payment transactions. However, throughout 2020, the share of digital-wallet usage increased significantly to 44%.[5]

b. Lending

Fintech Lending—also known as Fintech Peer-to-Peer Lending or Information Technology–Based Joint Funding Services (LPBBTI)—is a financial-sector innovation that utilizes technology to enable lenders and borrowers to conduct lending transactions without having to meet in person. The lending mechanism is facilitated through a system provided by the Fintech Lending Operator, either through an application or a website. Fintech Lending Operators function solely as intermediaries that connect lenders and borrowers. Both lenders and borrowers must first register and provide the required personal information before they can offer or apply for loans.

According to data from the Financial Services Authority (FSA), there are 102 licensed information technology–based joint funding service providers operating in Indonesia. As of June 2023, FSA has shut down 4,148 unlicensed ones.

[5] Bank Indonesia. 31 March 2023. *"Digital Wallets on the Rise, Attracting Interest During the Pandemic."* https://www.bi.go.id/id/bi-institute/BI-Epsilon/Pages/Dompet-Digital--Naik-Daun,-Membetot-Minat-Kala-Pandemi.aspx

Based on FSA data summarized in the Peer-to-Peer Lending Fintech Indicators,[6] the following are statistics for peer-to-peer lending fintech:

Table 1. Peer-to-Peer Lending Fintech Statistics

Component	Unit	2019	2020	2021	2022	2023 (as of Aug 2023)
Total Accumulated Lender Accounts	Accounts	605,935	716,963	809,494	999,455	1,077,223
Total Accumulated Borrower Accounts	Accounts	18,569,123	43,561,362	73,246,852	99,795,780	119,798,741
Total Accumulated Lender Transactions	Accounts	60,418,211	136,602,879	230,004,902	362,910,038	444,420,442
Total Accumulated Borrower Transactions	Accounts	81,876,033	248,407,423	533,121,562	722,496,413	833,101,406
Total Accumulated Loan Amount	Billion Rupiah	81,498	155,903	295,853	528,006	677,507

Source: Indonesian Financial System Statistics

c. Crowdfunding

Crowdfunding consists of four types: donation-based, reward-based, debt-based, and equity-based crowdfunding. In Indonesia, only debt-based, equity-based, and donation-based crowdfunding are subject to supervision and regulation, while reward-based crowdfunding does not fall under any supervisory or regulatory authority.

i. Donation-Based Crowdfunding

Donation-based crowdfunding is similar to conventional donation fundraising but is conducted online through websites or applications. As the name suggests, donation-based crowdfunding collects funds to be donated to those in need, typically for non-profit activities such as the construction of orphanages, schools, and similar initiatives. Donation-based crowdfunding platforms are generally established in the form of foundations and obtain permits for the collection of money and goods from the Ministry of Social Affairs. An example of a donation-based crowdfunding platform is kitabisa.com. According to data obtained from the Ministry of Social Affairs, there are 264 foundations licensed to collect money and goods[7].

[6] Bank Indonesia. (n.d.). *Indonesian Financial System Statistics.* Retrieved from https://www.bi.go.id/id/statistik/ekonomi-keuangan/sski/default.aspx#headingOne

[7] We submitted a data request regarding entities holding permits for Public Fundraising (PUB) to the Ministry of Social Affairs that also maintains websites. The data obtained did not indicate whether all foundations holding PUB permits have websites; however, we attempted to conduct sample searches

ii. Reward-Based Crowdfunding

In reward-based crowdfunding, an individual or a group submits a project proposal to be funded and typically offers rewards or incentives in the form of goods, services, or certain rights. This differs from debt-based or equity-based crowdfunding, as reward-based crowdfunding does not involve profit-sharing, returns, shares, or ownership stakes in the project. This type of crowdfunding is commonly used by creative industries such as music, gaming, fashion, and other arts. Examples of reward-based crowdfunding platforms include kickstarter.com, ko-fi.com, patreon.com, and buymeacoffee.com (international), as well as trakteer.id, karyakarsa.com, and saweria.co (domestic).[8]

Platforms such as kickstarter.com operate as Public Benefit Corporations, which are for-profit corporate entities whose objectives include generating positive social impact. In addition, for projects based in the United States that meet certain income thresholds, kickstarter.com issues Form 1099-K for tax-reporting purposes. No similar regulatory arrangements were identified in Indonesia. Based on our review of trakteer.id and karyakarsa.com, any taxes applicable to income earned by creators must be self-reported by the creators themselves. No equivalent provisions were identified on saweria.co.

iii. Debt-Based and Equity-Based Crowdfunding

In 2018, FSA issued Regulation No. 37/POJK.04/2018 concerning Equity Crowdfunding through Information Technology–Based Share Offerings. The concept is similar to share ownership, whereby invested funds become equity or ownership stakes in a company in return for dividends. Subsequently, equity crowdfunding evolved into securities crowdfunding (SCF) following the issuance of FSA Regulation No. 57/POJK.04/2020 on Securities Offerings through Information Technology–Based Crowdfunding Services (LUDBTI/Securities Crowdfunding/SCF). Information

and found that several samples do indeed have websites. In addition, we submitted a data request to the Ministry of Communication and Informatics (Kemenkominfo) regarding entities conducting crowdfunding activities under an Electronic System Operator (PSE) license. However, Kemenkominfo does not maintain data specifically identifying PSEs engaged in crowdfunding activities, as PSE data are categorized based on the Indonesian Standard Industrial Classification (KBLI). Search results from the website attached to our data request (https://pse.kominfo.go.id/home/pse-domestik) using the keyword “Foundation” (Yayasan) displayed 20 entries out of 14,129 entries, with the Health Sector, Information and Communication Technology Sector, and Trade Sector listed as the PSE sectors. In addition to the data obtained, there may be more donation-based crowdfunding activities on the internet, whether licensed or unlicensed. The data obtained do not include donation-based crowdfunding activities conducted through media other than websites or applications (for example, social media posts or offline/physical crowdfunding activities).

[8] To date, we have not been able to identify an official list of the number of reward-based crowdfunding platforms in Indonesia. There may be more reward-based crowdfunding platforms operating in Indonesia beyond those identified above.

Technology–Based Crowdfunding Services is a fundraising method based on a joint-investment scheme carried out by business owners to establish or expand their businesses. Investors may purchase and obtain ownership in the form of shares, debt securities (bonds), or collective ownership certificates (*sukuk*). Ownership interests are allocated in proportion to the value of each investor's contribution.

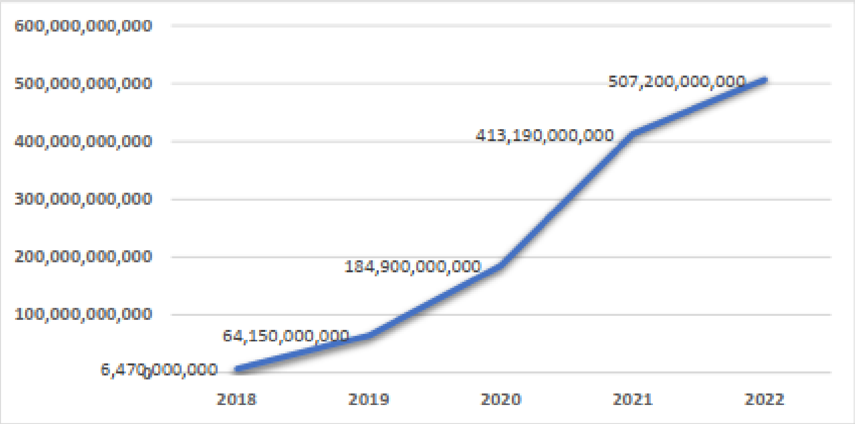


Figure 8. Funds Raised through LUDBTI, 2018–June 2022

Source: FSA, as cited in katadata.co.id

As of the first half of 2023, there were 16 LUDBTI companies licensed by FSA. In 2018, only around 1,380 investors invested their funds through LUDBTI; by mid-2022, this number had increased significantly to 111,351 investors. Based on FSA data compiled by katadata.co.id,[9] the following shows the development of funds raised by the LUDBTI industry from 2018 to June 2022.

Based on FSA data published in the Capital Market Statistics, First Half of 2023, the total number of issuers (fund recipients) from 2019 through the first half of 2023 was 419 issuers, while the number of investors reached 154,940. The total amount of funds disbursed from 2019 through the first half of 2023 amounted to IDR 892,094,482,250.

[9] Katadata.co.id. "Securities Crowdfunding Funds Reach IDR 507 Billion as of June 2022." https://databoks.katadata.co.id/datapublish/2022/06/09/dana-securities-crowdfunding-tembus-rp507-miliar-per-juni-2022

d. Investment

Fintech can be used for investment through various mechanisms. In practice, both Fintech Peer-to-peer Lending and LUDBTI may also serve as investment instruments in addition to their fundraising functions; however, in this SRA, fintech categorized under investment includes multi-asset investment applications, crypto assets, and digital gold.

Below are data on the number of fintech entities engaged in investment activities, based on the categories defined in this SRA.[10]

Table 2. Number of Financial Technology Providers in the Investment Sector

No.	Type of Investment Fintech	Number of Entities	Regulator
1	Multi-Asset Investment Applications	7[11]	Depending on the type of asset. Digital gold and crypto assets are regulated by Bappebti, while capital market investment products are regulated by FSA.
2	Digital Gold Traders	5	Bappebti
3	Prospective Physical Crypto Asset Traders[12]	32	Bappebti

[10] We have made efforts to compile a list of investment-related fintech; however, there remains the possibility that other types of investment fintech exist but were not identified in this SRA.

[11] We define multi-asset investment applications as investment applications that offer at least capital market investment products (such as shares, mutual funds, bonds, government securities, etc.), digital gold, and/or crypto assets. If an investment application offers only capital market products, it is not included in this category. We did not obtain an official list of multi-asset investment applications. The data were obtained from https://www.tanamduit.com/belajar/reksa-dana/aplikasi-investasi-reksadana, followed by manual searches to obtain further information on the investment applications. Of the 10 investment applications identified, three were excluded from the list: one platform offers only general capital market products, while the other two are wealth management platforms rather than investment applications that allow investors to independently purchase multiple asset classes. The number of multi-asset investment applications operating in Indonesia may therefore be greater than those identified in this SRA.

[12] As of now, crypto asset service providers officially operating in Indonesia are still referred to by Bappebti as prospective physical crypto asset traders, as they have not yet met the requirements to be designated as physical crypto asset traders.

2.3. SUPERVISION AND REGULATION OF FINANCIAL TECHNOLOGY IN INDONESIA

The supervision and regulation of fintech in Indonesia are carried out based on the nature of business activities. Bank Indonesia supervises and regulates fintech related to payments and fund transfers. Bappebti supervises and regulates fintech operating in the commodity futures trading sector, including crypto assets and digital gold. Other types of fintech are regulated by the Financial Services Authority (FSA). Fintech under FSA supervision includes *LPBBTI*, *LUDBTI*, and DFI. In accordance with Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector, the supervision and regulation of crypto assets will be transferred from Bappebti to FSA starting in 2025.

a. Regulations for Financial Technology Providers

Supervisory and Regulatory Authorities (SR Authorities) have the authority to supervise, regulate, and/or impose sanctions on Reporting Parties. In exercising these powers, SR Authorities issue regulations as the legal basis for supervision and enforcement. The following are regulations issued by each SR Authorities from 2018 to 2023 for financial technology providers under their respective supervision:

Table 3. FSA Regulations for Financial Technology Providers

No.	Regulation	Topic
1	POJK No. 23/POJK.01/2019	Amendment to Financial Services Authority Regulation No. 12/POJK.01/2017 on the Implementation of Anti-Money Laundering and Counter-Terrorist Financing Programs in the Financial Services Sector
2	POJK No. 8 of 2023	Implementation of Anti-Money Laundering, Counter-Terrorist Financing, and Prevention of Proliferation Financing of Weapons of Mass Destruction Programs in the Financial Services Sector
3	SEOJK No. 31/SEOJK.01/2019	Guidelines for Immediate Blocking of Customer Funds in the Financial Services Sector Identified in the List of Proliferation Financing of Weapons of Mass Destruction
4	SEOJK No. 6/SEOJK.05/2021	Guidelines for the Implementation of Anti-Money Laundering and Counter-Terrorist Financing Programs for Information Technology–Based Lending Service Providers
5	SEOJK No. 17/SEOJK.04/2022	Guidelines for the Implementation of Anti-Money Laundering and Counter-Terrorist Financing Programs for Information Technology–Based Crowdfunding Service Providers

Table 4. Bank Indonesia Regulations for Financial Technology Providers

No.	Regulation	Topic
1	PBI Number 22/23/PBI/2020	Payment Systems
2	Know Your Customer (Customer Due Diligence) Principles for Non-Bank Payment System Service Providers and Non-Bank Foreign Exchange Business Activities (2020)	Customer Due Diligence Principles
3	PBI Number 23/6/PBI/2021	Payment Service Providers
4	PADG No. 24/7/PADG/2022	Operation of Payment Systems by PJP and PIP

Table 5. Bappebti Regulations for Financial Technology Providers

No.	Regulation	Topic
1	Bappebti Regulation Number 6 of 2019	Implementation of AML/CFT Programs Related to the Operation of the Physical Commodity Market on Futures Exchanges
2	Bappebti Regulation Number 8 of 2021	Guidelines for the Operation of Crypto Asset Trading
3	Bappebti Regulation Number 13 of 2022	Amendment to Bappebti Regulation Number 8 of 2021
4	Bappebti Regulation Number 5 of 2023	Guidelines for the Prevention of Proliferation Financing of Weapons of Mass Destruction by Futures Brokers, Prospective Physical Crypto Asset Traders, and Physical Crypto Asset Traders
5	Bappebti Regulation Number 8 of 2023	Amendment to Bappebti Regulation Number 5 of 2023

b. The Role of Supervisory and Regulatory Agencies in Risk Mitigation Efforts

In addition to issuing regulations, Supervisory and Regulatory Agencies (SR Authorities) play a role in conducting supervision and imposing sanctions on service providers. SR Authorities is also authorized to designate official service provider associations, such as the Indonesian Fintech Association (AFTECH), the Indonesian Fintech Lending Association (AFPI), the Indonesian Sharia Fintech Lending Association (AFPSI), the Indonesian Payment Systems Association (ASPI), the Indonesian Blockchain Association (ABI), the Indonesian Equity Crowdfunding Association (ALUDI), and others. Furthermore, SR Authorities carry out socialization and outreach activities directed at both service providers and the public.

SR Authorities and other competent authorities also engage in cooperation and coordination through various task forces, including the Investment Alert Task Force (Satgas Waspada Investasi), which consists of 13 ministries/agencies, namely the Financial Services Authority (FSA) (as Chair and Secretariat), the Indonesian National Police, the Attorney General’s Office of the Republic of Indonesia, the Ministry of Trade, the Ministry of Cooperatives and Small and Medium Enterprises, the Ministry of

Communication and Informatics, the Ministry of Religious Affairs, the Ministry of Education, Culture, Research, and Technology, the Ministry of Home Affairs, Bank Indonesia, the Financial Transaction Reports and Analysis Center (INTRAC), and the Ministry of Investment/Investment Coordinating Board. The establishment of the Investment Alert Task Force aims to enhance coordination among ministries/agencies in preventing and addressing alleged unlawful activities in the field of public fund collection and investment management.

2.4. FATF RECOMMENDATIONS RELATED TO FINANCIAL TECHNOLOGY

One of the foundations of an effective AML/CFT regime is an adequate understanding of the risks of money laundering (ML), terrorist financing (TF), and proliferation financing of weapons of mass destruction (PF). Failure to identify, assess, and mitigate ML, TF, and PF risks may hinder the effectiveness of the AML/CFT regime. In this regard, FATF Recommendation 1 stipulates that countries must identify, assess, and understand their ML, TF, and PF risks and apply a risk-based approach (RBA). Countries must also require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess, and take effective measures to mitigate their ML, TF, and PF risks. As some financial technology providers qualify as financial institutions, they are required to implement FATF Recommendation 1.

In addition to Recommendation 1 (assessing risks and applying a risk-based approach), other FATF Recommendations relevant to financial technology include:

a. Recommendation 10 (customer due diligence)
b. Recommendation 11 (record keeping)
c. Recommendation 12 (politically exposed persons)
d. Recommendation 13 (correspondent banking)
e. Recommendation 14 (money or value transfer services)
f. Recommendation 15 (new technologies)
g. Recommendation 16 (wire transfers)
h. Recommendation 17 (reliance on third parties)
i. Recommendation 18 (internal controls and foreign branches and subsidiaries)
j. Recommendation 19 (higher-risk countries)
k. Recommendation 20 (reporting of suspicious transactions)
l. Recommendation 21 (tipping-off and confidentiality).

CHAPTER III RESEARCH METHODOLOGY

3.1. RESEARCH METHOD

The research methodology used in the 2023 Fintech SRA is a mixed-method explanatory sequential design. This methodology combines qualitative and quantitative research methods in a sequential manner. The quantitative approach utilizes statistical data derived from suspicious financial transaction reports, supervisory activities, FIU information exchange, financial intelligence reports, investigations, prosecutions, and court judgments. Meanwhile, the qualitative approach is based on self-assessments conducted by experts from reporting entities, supervisory and regulatory authorities, the financial intelligence unit (INTRAC), and law enforcement apparatus regarding the quality of preventive and enforcement aspects related to money laundering and terrorist financing crimes in the financial technology sector.

The guidelines used in preparing the 2023 Fintech SRA refer to international best practices, including the National Money Laundering and Terrorist Financing Risk Assessment (FATF Guidance), Risk Assessment Support for Money Laundering/Terrorist Financing (World Bank), Review of the Fund’s Strategy on Anti-Money Laundering and Combating the Financing of Terrorism (IMF), and the Terrorist Financing Risk Assessment Guidance.

3.2. SCOPE AND STEPS OF RISK ASSESSMENT

The scope of the 2023 Fintech SRA includes the identification of types of financial technology operating in Indonesia; the identification and analysis of ML and TF risks associated with different types of fintech, covering predicate offenses for money laundering, ML and TF typologies, geographic areas or provinces, and offender profiles; as well as the identification of potential risks of fintech misuse for election campaign financing. The FATF Guidance explains that risk is formulated as a function of the following elements:

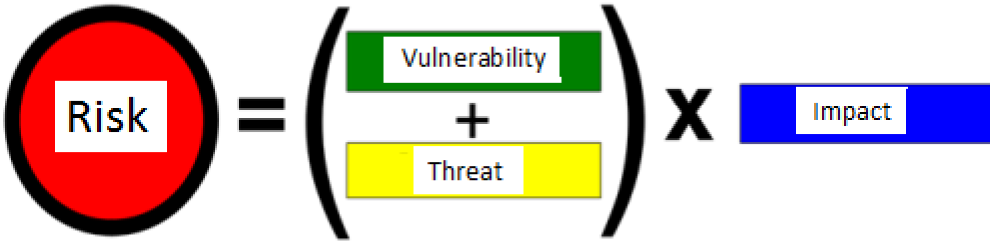


Figure 9 Risk Assessment Formulation

a. **Threat**, refers to a person or group of persons, objects, or activities that have the potential to cause harm, for example to the state, society, the economy, and others. In the context of ML/TF, this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present, and future ML or TF activities.

b. **Vulnerability**, refers to factors that can be exploited by threats or that may support or facilitate their activities. In the context of ML/TF risk assessment, viewing vulnerabilities as distinct from threats means focusing on, for example, factors that represent weaknesses in the AML/CFT system or controls, or specific characteristics within a country. This may also include features of particular sectors, financial products, or types of services that make them attractive for ML or TF purposes.

c. **Likelihood**, refers to the probability or chance of the occurrence of money laundering and terrorist financing activities.

d. **Consequence/impac**, refers to the impact or harm that may be caused by ML or TF and includes the effects of the underlying criminal and terrorist activities on financial systems and institutions, as well as on the economy and society in general. The consequences of ML or TF may be short-term or long-term and may also relate to specific populations or communities, the business environment, national or international interests, as well as the reputation and attractiveness of a country's financial sector.

e. **Emerging Trend**, refers to a channel or pathway that is newly emerging and/or developing as a means of money laundering and terrorist financing before its impact becomes widespread.

3.3. STAGES OF RISK ASSESSMENT

In preparing the 2023 Fintech SRA, several stages of activities were carried out throughout 2023, as follows:

I. Preparation Stage

1. Establishment of internal and external teams for the preparation of the 2023 Fintech SRA in May 2023.
2. Meetings with regulators, law enforcement apparatus, and relevant ministries/agencies regarding the urgency of preparing the Fintech SRA in July 2023.

II. Implementation Stage

a. Risk Identification

At this stage, the process involves identifying risk factors to be analyzed, as well as identifying the types of data and information required.

b. Risk Analysis

The risk analysis stage is a continuation of the risk identification stage, using the variables of vulnerability, threat, and consequence. The purpose of this step is to analyze the identified risk factors in order to understand their nature, sources, likelihood, and consequences, and to determine relative risk levels for each risk factor.

c. Risk Evaluation

This stage involves the process of drawing conclusions from the findings obtained during the analysis stage to determine priorities in addressing risks, taking into account the objectives of the risk assessment at the outset of the process. This stage also contributes to the development of risk mitigation strategies aimed at addressing identified risks.

III. Launch or Dissemination Stage

The launch or dissemination stage is carried out to provide understanding and to raise shared awareness regarding sectoral ML and TF risks in the fintech sector. The implementation of the launch or dissemination includes:

1. Finalization of the report.
2. Launch and communication of the results of the 2023 Fintech SRA Report to regulators, law enforcement apparatus, and relevant ministries/agencies.

3.4. DATA SOURCES

The preparation of the 2023 Fintech SRA was conducted using data covering the period from 2019 to June 2023. The quantitative approach utilizes statistical data sourced from statistics on suspicious financial transaction reports, supervisory activities, FIU information exchange, financial intelligence reports, investigations, prosecutions, and court decisions. Meanwhile, the qualitative approach relies on self-assessments conducted by experts representing reporting entities, supervisory and regulatory authorities, the financial intelligence unit (INTRAC), and law enforcement apparatus. All such data and information were used to identify, analyze, and evaluate the risks of money laundering and terrorist financing related to fintech.

Qualitative data collection was carried out by distributing questionnaires to supervisory and regulatory authorities, law enforcement apparatus, relevant ministries/agencies, and reporting entities, involving a total of 20 respondents with an average response rate of 95%, as detailed below:

a. 3 respondents from 3 supervisory and regulatory authorities, with an average response rate of 100%;
b. 5 respondents from 6 law enforcement apparatus, with an average response rate of 83%;
c. 1 respondent from 2 relevant ministries/agencies, with an average response rate of 50%;
d. 11 respondents from 11 reporting entities, with an average response rate of 100%.

In addition to questionnaires, data were also collected through interviews with 3 representatives of supervisory and regulatory authorities, 4 representatives of law enforcement apparatus, and 11 representatives of reporting entities to obtain deeper insights into ML and TF risks in the fintech sector. The topics discussed in the SRA questionnaires and interviews included, among others:

Table 6. SRA Questionnaire and Interview Topics

Questionnaire	Interview
1. Perceptions of ML and TF threats, vulnerabilities, and impacts by fintech type (PoC) 2. Number and nominal value of cases (investigation, prosecution, court decisions) of ML and TF involving fintech by type (law enforcement only) 3. Perceptions of threats, vulnerabilities, and impacts of fintech misuse for election campaign financing 4. Case studies 5. List of licensed and unlicensed service providers (supervisory authorities only)	1. Perceptions of ML and TF threats, vulnerabilities, and impacts related to fintech compared to conventional financial institutions and DNFBPs 2. Perceptions of fintech ML/TF risk mitigation capacity: a. Reporting entities' capacity to comply with AML/CFT obligations b. Supervisory authorities' capacity to supervise and regulate fintech c. Law enforcement apparatus' capacity to handle ML and TF cases involving fintech 3. Emerging ML and TF threats related to fintech 4. Suspicious financial transaction indicators in fintech 5. Forms of domestic and international cooperation (law enforcement apparatus and supervisory authorities only) 6. Challenges: a. Compliance with AML/CFT obligations (reporting entities) b. AML/CFT supervision (supervisory authorities) c. Supervisors' perceptions of challenges in AML/CFT compliance by reporting entities d. Case handling (law enforcement apparatus) 7. Recommendations: a. Prevention b. Enforcement c. Cooperation 8. Potential misuse of fintech in elections

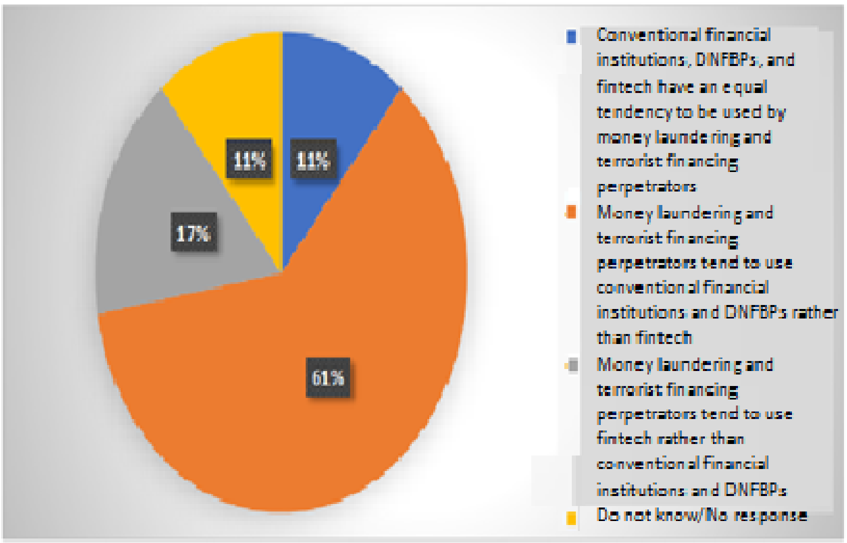
CHAPTER IV RISK ASSESSMENT RESULTS

4.1. INTERVIEW RESULTS

a. Threats, Vulnerabilities, and Impacts of Financial Technology Compared with “Conventional” Financial Institutions and DNFBPs

We asked respondents about their general perceptions regarding the tendency for fintech to be used in ML and TF, the level of supervision and regulation of fintech in relation to AML/CFT compliance, and the impacts that would arise if ML and TF occurred in fintech, compared with “conventional” financial institutions and DNFBPs[13]. Overall, 61% of respondents tended to believe that criminals are more likely to use “conventional” financial institutions and DNFBPs to conduct ML and TF. This perception was relatively evenly distributed across respondent categories (law enforcement apparatus 75%, supervisory and regulatory authorities 67%, and reporting entities 54%). Furthermore, compared with conventional financial institutions and DNFBPs, the majority of respondents (73%) were of the view that supervision and regulation of fintech are already adequate. With regard to impact, 50% of respondents believed that the impact of ML and TF would be greater if such crimes occurred in fintech than in “conventional” financial institutions and DNFBPs.

Figure 10 Respondents’ Perceptions of the Tendency for Fintech to Be Used by ML/TF Perpetrators Compared with “Conventional” Financial Institutions and DNFBPs



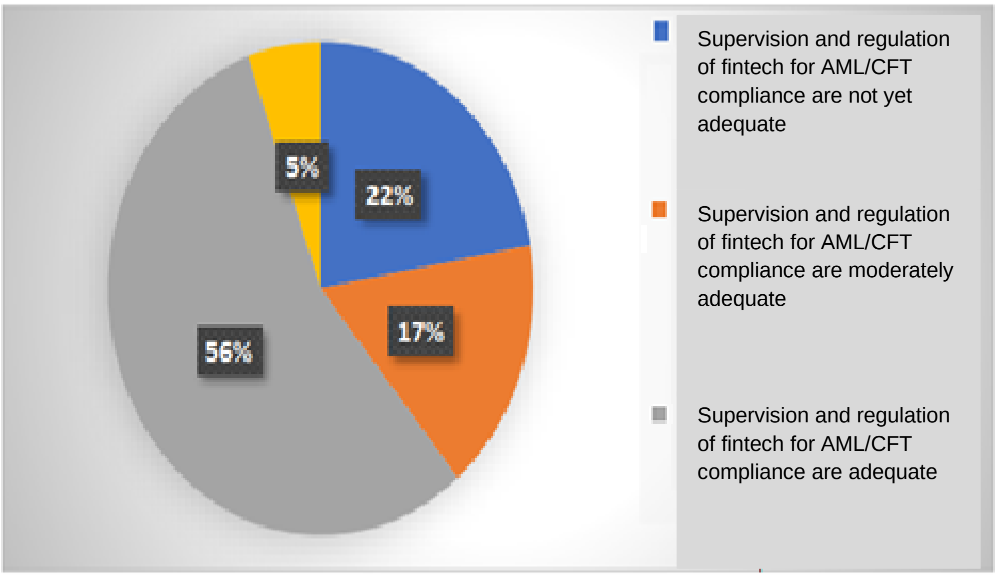
[13] Reporting parties classified as fintech include, but are not limited to: issuers of e-money and/or e-wallets (excluding electronic money card providers); providers of money remittance business activities (not all providers, but only those operating through web-based platforms and/or applications); providers of information technology–based peer-to-peer lending services; providers of equity crowdfunding services through information technology–based share offerings; and providers of information technology–based financial transaction services. Other reporting parties outside these categories are classified as “conventional” Financial Institutions and DNFBPs.

Respondents' reasons for believing that ML and TF perpetrators are more likely to use "conventional" financial institutions and DNFBPs rather than fintech include, among others:

a. Fintech is a relatively new technology and may not yet be easily used by everyone. In addition, several types of fintech impose transaction limits. Fintech e-wallets, e-money, and remittance services generally have lower transaction limits compared with bank fund transfers, although for other types of fintech the transaction limits can be relatively high. Moreover, regulatory requirements for certain types of fintech are quite stringent. For fintech providers, SR Authorities also function as licensing or operational permit–issuing authorities, which leads fintech to be perceived as more compliant with SR Authorities requirements than DNFBPs.

b. Most ML and TF cases identified to date still involve "conventional" financial institutions and DNFBPs rather than fintech. However, there is a possibility that this trend may change in the future.

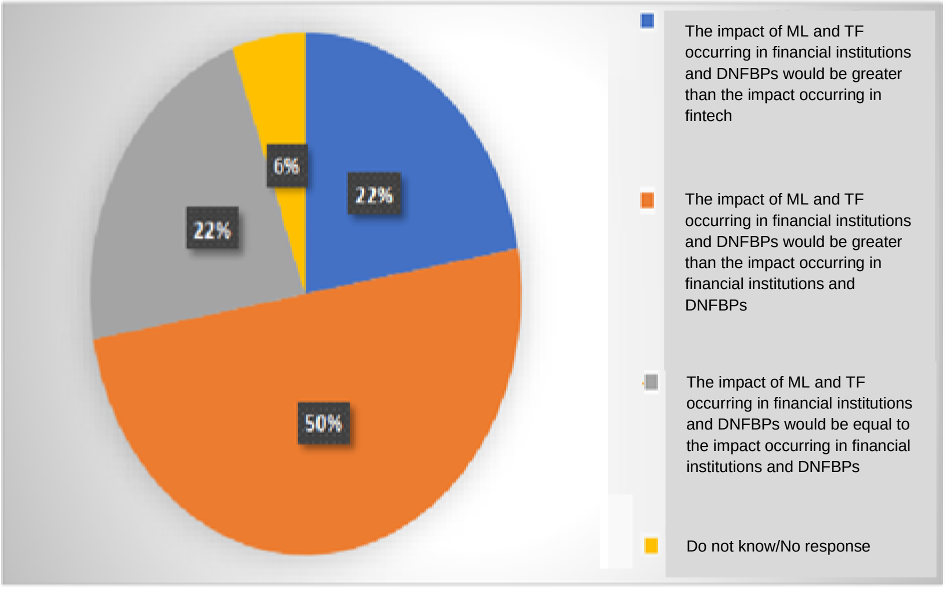
Figure 11 Respondents' Perceptions of AML/CFT Supervision and Regulation of Fintech Compared with "Conventional" Financial Institutions and DNFBPs



The implementation of AML/CFT requirements in fintech is considered to be more stringent than in "conventional" financial institutions and DNFBPs because fintech already utilizes the latest technologies, such as integration with population databases and biometric data, including facial recognition technology. In addition, for crypto asset service providers, there are several software tools capable of monitoring transactions, such as Chainalysis. From a supervisory and regulatory perspective, both on-site and off-site supervision are conducted, along with obligations to submit periodic reports to SR Authorities.

Although most respondents consider supervision and regulation of fintech to be adequate, law enforcement apparatus (LEAs) noted that gaps in fintech supervision and regulation still exist. These gaps include fintech entities that only register as Electronic System Providers (PSEs) and do not register with the relevant SR Authorities. This modus operandi is commonly used by illegal fintech operators that operate through websites. Furthermore, there are several illegal fintech entities that closely resemble licensed fintech providers, for example by using similar logos with different colors, thereby misleading users. The lack of global regulatory standardization for crypto assets also allows for regulatory shopping, whereby users tend to choose service providers that are less regulated or not well regulated, particularly across different jurisdictions.

Figure 12 Respondents' Perceptions of the Impact of ML and TF Occurring in Fintech Compared with "Conventional" Financial Institutions and DNFBPs



Regarding impact, respondents tend to be of the view that the impact arising from ML and TF occurring in fintech would be greater than that occurring in "conventional" financial institutions and DNFBPs. For respondents who consider the impact of fintech to be greater, the reasons include the relatively large transaction values in crypto-asset fintech and the generally faster transaction velocity in fintech. In addition, there is the possibility of both domestic and cross-border transactions. Law enforcement apparatus are of the view that asset tracing and recovery, as well as evidentiary processes for ML and TF in fintech, are relatively challenging due to limited resources, particularly investigators' lack of knowledge and expertise in fintech.

b. Capacity to Mitigate ML and TF Risks in Fintech

i. Capacity of Reporting Entities to Comply with AML/CFT Requirements

Based on the sample of reporting entities, consisting of 3 payment system service providers (PSP), 4 fintech peer-to-peer lending providers, 2 prospective physical crypto-asset traders, and 2 multi-asset investment applications, all reporting entities have established standard operating procedures (SOPs related to AML/CFT). In addition, all sampled reporting entities have transaction monitoring systems in place. Furthermore, all sampled reporting entities have received outreach from regulators, including the issuance of regulations, education and training, audits, and the dissemination of sanctions lists such as the List of Suspected Terrorists and Terrorist Organizations and the Proliferation Financing Sanctions List. In addition, several sampled reporting entities have taken the initiative to incorporate additional sanctions lists (such as WorldCheck and the OFAC List) into their systems, conduct in-house training, and participate in Compliance and AML certification programs

.

According to the perception of supervisory and regulatory authorities (SR Authorities), fintech's risk mitigation capacity is generally adequate due to the adoption of up-to-date technology, relatively moderate transaction values, comprehensive transaction recording within systems, and compliance personnel who are often former employees of "conventional" financial institutions and DNFBPs, thereby possessing greater experience in implementing AML/CFT requirements. Nevertheless, SR Authorities noted several challenges faced by fintech in complying with AML/CFT obligations, including difficulties in determining predicate offenses when reporting suspicious transaction reports (STRs), incomplete connectivity of reporting entities to population data held by the Directorate General of Population and Civil Registration, uneven understanding between ML and TF risks, the inability of some fintech providers to detect beneficial owners in virtual account transactions, and high turnover of AML/CFT personnel.

According to the perception of law enforcement apparatus, the risk mitigation capacity of licensed fintech providers is also considered adequate, but only for licensed fintech entities that fall under SR Authorities supervision. Unlicensed fintech entities are difficult to trace in the event of criminal activity, as they tend to be uncooperative in providing data and information.

ii. Capacity of Supervisory and Regulatory Authorities to Supervise and Regulate Fintech

From a supervisory perspective, the Financial Services Authority (FSA) has dedicated supervisors for reporting entities operating as fintech providers. Bank Indonesia (BI) and Bappebti do not have dedicated supervisors for fintech reporting entities, as supervision has historically been conducted based on business activities; fintech under BI and Bappebti generally conducts similar or equivalent business activities, differing primarily in the use of new technology. Meanwhile, fintech entities under FSA supervision engage in business activities that differ more significantly from those of "conventional" financial institutions.

SR Authorities also issue regulations (as discussed in Chapter II) and conduct outreach activities for reporting entities under their supervision. Such outreach includes socialization activities, education and training programs, and audits.

Forms of cooperation in AML/CFT supervision and regulation undertaken by SR Authorities include both domestic and international cooperation. Domestic cooperation includes memoranda of understanding (MoUs) between each SR Authorities and relevant ministries/agencies, MoUs with law enforcement apparatus, cooperation with fintech industry associations, and participation in the Investment Alert Task Force (as discussed in Chapter II). The scope of this cooperation includes AML/CFT training, the development of fintech data centers, preparation of sectoral risk assessments, cooperation in drafting AML/CFT regulations, information exchange, handling of illegal fintech cases, and cooperation in licensing processes. International cooperation includes MoUs with foreign counterparts (such as central banks or financial services authorities of other countries), cooperation with international organizations such as UNODC and the Asia/Pacific Group on Money Laundering, and cooperation with foreign government institutions such as the US Embassy.

The scope of such cooperation includes AML/CFT training, knowledge sharing, and information exchange.

iii. Capacity of Law Enforcement Apparatus in Handling ML and TF Cases Involving Fintech

Although law enforcement apparatus (LEA) do not have investigators specifically assigned to handle fintech-related cases, in principle all investigators are authorized to investigate cases involving fintech. From the perspective of internal policy, there are general standard operating procedures (SOPs) for case handling; however, there are no SOPs specifically tailored to fintech cases. Fifty percent of the sampled investigators (2 out of 4 investigators) stated that they had participated in fintech-related education and training within the past five years.

Forms of cooperation in handling ML and TF cases include domestic cooperation through memoranda of understanding (MoUs) with relevant ministries/agencies, as well as cooperation with reporting entities and industry associations, with the scope covering information exchange and education and training. International cooperation includes cooperation with foreign authorities, with scopes that include information exchange and mutual legal assistance (MLA).

4.2. RISK ASSESSMENT

In conducting the risk assessment, three factors must be considered, namely threats, vulnerabilities, and impact. We combined the results of the questionnaires (perceptions) with quantitative data in the form of Suspicious Financial Transaction Reports (STRs), financial intelligence products, public complaints, expert testimony, investigations, prosecutions, and court decisions (where available) to obtain the risk assessment results. Based on field findings, most cases involving fintech are predicate offense (PO) cases (for example, fraud and embezzlement), and there have not yet been many cases of money laundering (ML) and terrorist financing (TF). Therefore, caution is required in interpreting the results of this fintech SRA, as most of the data obtained are still based on perceptions and intelligence products. The following presents the results of the risk assessment for each point of concern (PoC) for each type of fintech covered in this SRA.

a. Type of Fintech

The types of fintech assessed as having a high ML risk are **investment** and **remittance and payment**. One ML court decision related to investment fintech was identified and will be discussed in the section on Typologies and Case Studies, while no ML court decisions have yet been identified for remittance and payment fintech. Investment fintech is used by perpetrators to place the proceeds of crime through the purchase of crypto assets, based on the identified ML court decision. Remittance and payment fintech are generally used to transfer funds, whether legitimate or illicit.

Table 7 Risk of Money Laundering by Type of Fintech

Type of Fintech	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Investment	9.00	3.00	9.00	9.00	HIGH
Remittance and Payment	6.32	6.48	4.72	5.64	MEDIUM
Crowdfunding	3.00	9.00	4.83	5.58	MEDIUM
Lending	3.32	4.79	3.00	3.00	LOW

With regard to terrorist financing (TF), the type of fintech assessed as having a high risk is lending. There are two TF court decisions in which online lending platforms, both licensed and unlicensed, were used by terrorist financing perpetrators to raise funds. There is also the possibility that crypto assets are used to store terrorist funds; in other jurisdictions, there have been cases involving fraudulent donation schemes in which the proceeds were subsequently converted into crypto assets. Remittance and payment services may be used to transfer funds for terrorist purposes, although no court decisions involving fintech-based remittance and payment services have been identified in Indonesia to date. Existing TF cases in Indonesia involving remittance and payment services still fall within conventional remittance and payment channels and do not yet involve fintech. Similar to remittance and payment services, crowdfunding also has the potential to be misused for terrorist financing, although no court decisions have been identified in Indonesia. Several cases abroad indicate that socially oriented fintech crowdfunding platforms are suspected of having been used for terrorist financing.

Table 8 Risk of Terrorist Financing by Type of Fintech

Type of Fintech	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Lending	9.00	3.00	9.00	9.00	HIGH
Investment	7.01	5.09	7.05	6.78	MEDIUM
Remittance and Payment	4.15	7.28	6.26	5.22	MEDIUM
Crowdfunding	3.00	9.00	3.00	3.00	LOW

b. Predicate Offences of Money Laundering

In general, the predicate offence (PO) with the highest risk across the four types of fintech is fraud. Embezzlement, gambling, and corruption are classified as medium-risk predicate offences. Embezzlement is the predicate offence most frequently identified in suspicious transaction reports (STRs) related to fintech, while fraud and terrorism are most frequently identified in INTRAC's financial intelligence products. Fraud is also the predicate offence most frequently identified in public complaints and in expert testimonies provided by INTRAC. At least one money laundering conviction, two terrorist financing convictions, and one predicate offence conviction involving fintech were identified and will be discussed further in the section on

Typologies and Case Studies. Examples of predicate offence cases involving fintech related to fraud and embezzlement include:

1. Misuse of the names of illegal online lending platforms. In this case, illegal online lending platforms replicate and misuse the names of legal platforms, causing members of the public to become victims of illegal online lending schemes. Fraud and embezzlement involving trading robots.
2. Trading robots are computer software programs that operate automatically to monitor markets, calculate entry opportunities, and manage risk based on algorithms embedded in their programming. Fraud or embezzlement in trading robot schemes typically involves the inability to withdraw investment funds or the implementation of Ponzi schemes. Examples of trading robot fraud cases include Auto Trade Gold (ATG), DNA Pro, Net89, Viral Blast, and Fahrenheit.

Table 9 High-Risk Predicate Offences Related to Fintech

Type of Predicate Offence (Money Laundering)	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Fraud	9.00	6.93	9.00	9.00	HIGH
Embezzlement	4.61	6.02	6.77	5.59	MEDIUM
Gambling	4.67	9.00	5.64	5.25	MEDIUM
Corruption	4.47	8.20	4.99	4.74	LOW
Narcotics	4.00	8.22	4.10	4.11	LOW
Psychotropics	3.84	7.99	3.89	3.94	LOW
Prostitution	3.65	5.29	3.79	3.65	LOW
Theft	3.52	5.37	3.70	3.58	LOW
Capital Market–Related Offences	3.55	6.71	3.51	3.58	LOW
Bribery	3.68	5.93	3.52	3.56	LOW
Other Offences Punishable by ≥4 Years Imprisonment	3.50	3.57	3.82	3.51	LOW
Banking Sector–Related Offences	3.58	3.64	3.75	3.50	LOW
Taxation Sector–Related Offences	3.41	6.32	3.45	3.49	LOW
Customs	3.34	4.32	3.35	3.30	LOW
Excise	3.34	4.29	3.35	3.30	LOW
Trafficking in Persons	3.26	4.52	3.21	3.23	LOW
Insurance Sector–Related Offences	3.29	3.00	3.19	3.13	LOW
Smuggling of Migrant Workers	3.13	3.77	3.15	3.12	LOW
Environmental Crimes	3.08	3.23	3.24	3.12	LOW
Forestry Sector–Related Offences	3.08	3.23	3.24	3.12	LOW

Migrant Smuggling	3.13	3.76	3.15	3.12	LOW
Marine and Fisheries Sector–Related Offences	3.08	3.23	3.21	3.11	LOW
Kidnapping	3.05	3.64	3.12	3.09	LOW
Counterfeiting of Currency	3.00	3.32	3.00	3.00	LOW

i. Payment and Remittance

Based on respondents' perceptions, Suspicious Financial Transaction Reports (STRs), and financial intelligence data related to payment and remittance services, the predicate offences (PO) considered to pose a high risk are gambling and corruption. No court rulings on money laundering offences related to payment and remittance fintech have been identified over the past five years.

Table 10 High-Risk Predicate Offences Related to Payment and Remittance Fintech

Type of Predicate Offence (Money Laundering)	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Fraud	9.00	6.15	9.00	9.00	HIGH
Corruption	4.47	8.54	7.93	7.22	HIGH
Narcotics	4.52	9.00	7.31	6.99	MEDIUM
Prostitution	3.98	8.98	6.94	6.56	MEDIUM
Psychotropics	3.79	8.84	6.57	6.22	MEDIUM
Banking Sector–Related Offences	4.59	3.22	8.54	5.80	MEDIUM
Other Offences Punishable by ≥4 Years Imprisonment	4.15	3.55	8.21	5.58	MEDIUM
Gambling	4.15	3.34	7.92	5.38	MEDIUM
Theft	3.20	3.42	7.15	4.72	LOW
Kidnapping	3.79	8.47	3.73	4.44	LOW
Capital Market–Related Offences	3.49	6.77	3.43	3.89	LOW
Forestry Sector–Related Offences	3.37	7.08	3.36	3.88	LOW
Bribery	3.59	6.26	3.43	3.81	LOW
Counterfeiting of Currency	3.71	6.20	3.35	3.79	LOW
Taxation Sector–Related Offences	3.55	5.83	3.33	3.68	LOW
Customs	3.28	4.54	3.26	3.36	LOW
Excise	3.28	4.50	3.26	3.35	LOW
Trafficking in Persons	3.20	4.69	3.09	3.29	LOW
Embezzlement	3.32	4.74	3.00	3.28	LOW

Smuggling of Migrant Workers	3.06	4.00	3.03	3.11	LOW
Migrant Smuggling	3.06	4.00	3.03	3.11	LOW
Marine and Fisheries Sector–Related Offences	3.00	3.55	3.14	3.07	LOW
Environmental Crimes	3.00	3.55	3.14	3.07	LOW
Insurance Sector–Related Offences	3.23	3.00	3.09	3.00	LOW

ii. Lending

Based on respondents' perceptions and Suspicious Financial Transaction Report (STR) data, narcotics, fraud, and gambling are considered high-risk predicate offences (PO). No money laundering (ML) cases related to lending fintech were identified during the 2019–2023 period. As previously noted, two court rulings on terrorist financing (TF) related to lending were identified.

Table 11 High-Risk Predicate Offences Related to Lending Fintech

Type of Predicate Offence (Money Laundering)	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Narcotics	4.76	6.79	7.00	7.77	HIGH
Fraud	9.00	5.56	5.95	9.00	HIGH
Gambling	4.70	3.45	9.00	8.78	HIGH
Other Offences Punishable by ≥4 Years Imprisonment	5.50	3.00	6.76	7.28	HIGH
Corruption	4.15	9.00	3.89	4.90	LOW
Bribery	3.69	6.31	3.36	3.89	LOW
Psychotropics	3.79	7.06	3.40	4.05	LOW
Smuggling of Migrant Workers	3.07	3.60	3.00	3.04	LOW
Migrant Smuggling	3.07	3.60	3.00	3.04	LOW
Banking Sector–Related Offences	3.31	4.35	3.07	3.27	LOW
Capital Market–Related Offences	3.49	7.06	3.32	3.87	LOW
Insurance Sector–Related Offences	3.23	3.45	3.00	3.08	LOW
Customs	3.26	4.80	3.18	3.39	LOW
Excise	3.26	4.80	3.18	3.39	LOW
Trafficking in Persons	3.23	4.20	3.07	3.23	LOW
Kidnapping	3.68	7.49	3.64	4.27	LOW
Theft	3.00	3.75	3.07	3.09	LOW
Embezzlement	3.39	6.46	3.04	3.52	LOW
Counterfeiting of Currency	3.84	7.81	3.47	4.22	LOW
Prostitution	3.88	8.48	3.67	4.51	LOW
Taxation Sector–Related Offences	3.26	4.96	3.22	3.44	LOW
Forestry Sector–Related Offences	3.30	5.71	3.29	3.60	LOW
Environmental Crimes	3.00	3.00	3.07	3.00	LOW

Marine and Fisheries Sector–Related Offences	3.00	3.00	3.07	3.00	LOW

iii. Crowdfunding

No money laundering (ML) or terrorist financing (TF) cases related to crowdfunding fintech were identified during the 2019–2023 period. Based on respondents' perceptions and Suspicious Financial Transaction Report (STR) data, fraud is considered the high-risk predicate offence (PO) for crowdfunding.

Table 12 High-Risk Predicate Offences Related to Crowdfunding Fintech

Type of Predicate Offence (Money Laundering)	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Fraud	9.00	7.59	9.00	9.00	HIGH
Corruption	4.22	9.00	3.78	4.01	LOW
Kidnapping	3.84	8.39	3.71	3.83	LOW
Counterfeiting of Currency	4.01	9.00	3.51	3.81	LOW
Prostitution	3.72	8.23	3.45	3.66	LOW
Narcotics	3.86	7.08	3.45	3.62	LOW
Psychotropics	3.87	7.06	3.38	3.58	LOW
Bribery	3.85	6.53	3.38	3.54	LOW
Capital Market–Related Offences	3.59	7.59	3.34	3.53	LOW
Forestry Sector–Related Offences	3.43	6.18	3.31	3.39	LOW
Embezzlement	3.51	6.88	3.07	3.33	LOW
Customs	3.35	4.76	3.20	3.23	LOW
Excise	3.35	4.76	3.20	3.23	LOW
Taxation Sector–Related Offences	3.29	4.76	3.17	3.20	LOW
Banking Sector–Related Offences	3.43	4.41	3.10	3.18	LOW
Trafficking in Persons	3.22	4.06	3.10	3.11	LOW
Insurance Sector–Related Offences	3.32	3.35	3.03	3.06	LOW
Theft	3.00	3.71	3.10	3.04	LOW
Gambling	3.11	3.71	3.00	3.02	LOW
Environmental Crimes	3.08	3.00	3.10	3.01	LOW
Marine and Fisheries Sector–Related Offences	3.08	3.00	3.10	3.01	LOW
Smuggling of Migrant Workers	3.06	3.35	3.03	3.00	LOW
Migrant Smuggling	3.06	3.35	3.03	3.00	LOW
Other Offences Punishable by ≥4 Years Imprisonment	3.08	3.00	3.07	3.00	LOW

iv. Investment

For the fintech investment category, the predicate offence (PO) assessed as high risk based on respondents' perceptions and STR data is fraud. No money laundering (ML) or terrorist financing (TF) cases related to investment fintech were identified in Indonesia during the period 2019–2023.

Table 13 High-Risk Predicate Offences Related to Investment Fintech

Predicate Offence	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Fraud	9.00	5.74	9.00	9.00	High
Embezzlement	5.01	4.71	6.78	5.67	Medium
Corruption	4.28	9.00	3.87	4.19	Low
Gambling	3.84	3.17	4.96	4.13	Low
Prostitution	4.01	7.58	4.02	4.08	Low
Counterfeiting of Currency	3.93	7.80	3.44	3.76	Low
Kidnapping	3.73	6.47	3.60	3.69	Low
Psychotropic Substances	3.90	7.46	3.38	3.69	Low
Narcotics	3.85	7.10	3.42	3.68	Low
Bribery	3.84	5.40	3.38	3.52	Low
Capital Market Crimes	3.55	6.43	3.34	3.51	Low
Forestry Crimes	3.31	6.09	3.30	3.41	Low
Theft	3.12	3.69	3.68	3.36	Low
Other Crimes Punishable by Imprisonment of 4 Years or More	3.22	3.00	3.70	3.34	Low
Customs Violations	3.29	4.71	3.19	3.25	Low
Excise	3.29	4.71	3.19	3.25	Low
Taxation Crimes	3.31	4.71	3.15	3.23	Low
Banking Crimes	3.31	3.86	3.08	3.13	Low
Human Trafficking	3.24	4.03	3.08	3.13	Low
Insurance Crimes	3.24	3.34	3.00	3.05	Low
Labor Smuggling	3.10	3.34	3.00	3.01	Low
Migrant Smuggling	3.10	3.34	3.00	3.01	Low
Environmental Crimes	3.00	3.00	3.08	3.00	Low
Marine and Fisheries Crimes	3.00	3.00	3.08	3.00	Low

c. Money Laundering Typologies

In general, the money laundering (ML) typologies considered to pose a high risk in fintech include asset purchases (such as property, vehicles, crypto assets, and others), structuring, and smurfing.

Table 14 High-Risk Money Laundering Typologies in Fintech

ML Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Asset purchases (property, vehicles, crypto assets, etc.)	6.94	8.49	8.49	9.00	HIGH
Structuring (breaking transactions into smaller amounts by a single individual)	6.38	9.00	6.41	7.50	HIGH
Smurfing (breaking transactions carried out by multiple individuals)	6.30	8.76	6.34	7.30	HIGH
Luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.)	6.02	8.16	5.89	6.61	MEDIUM
Mingling (mixing legitimate and illicit funds)	9.00	3.00	9.00	6.47	MEDIUM
Third-party account control/use of nominees	6.79	3.00	8.76	5.43	MEDIUM
Use of unlicensed service providers	5.40	3.00	3.00	3.35	LOW
Pass-by (funds withdrawn or re-transferred immediately after transfer)	3.85	3.00	3.00	3.12	LOW
Use of shell companies	3.00	3.00	3.00	3.00	LOW
Use of false or stolen identity data	3.00	3.00	3.00	3.00	LOW
Transfers to or receipt of funds from high-risk jurisdictions	3.00	3.00	3.00	3.00	LOW

i. Payments and Remittances

For fintech payments and remittances, the high-risk money laundering typologies are structuring, smurfing, and asset purchases (property, vehicles, crypto assets, etc.).

Table 15 High-Risk Money Laundering (ML) Typologies in Fintech Payments and Remittances

ML Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Structuring (splitting transactions into smaller amounts but conducted repeatedly by the same individual)	9.0	9.0	9.0	9.0	HIGH
Smurfing (splitting transactions conducted by multiple individuals)	8.88	8.21	8.88	8.42	HIGH
Asset purchases (property, vehicles, crypto-assets, etc.)	8.42	8.28	8.42	7.83	HIGH
Purchase of luxury goods (jewelry, gold, luxury bags, luxury cars, etc.)	8.3	6.37	8.08	6.63	MEDIUM
Use of shell companies	3.0	3.0	3.0	3.0	LOW
Third-party account control / use of nominees	3.0	3.0	3.0	3.0	LOW
Use of false or stolen identity data	3.0	3.0	3.0	3.0	LOW
Use of unlicensed service providers	3.0	3.0	3.0	3.0	LOW
Sending or receiving funds from high-risk jurisdictions	3.0	3.0	3.0	3.0	LOW
Mingling (mixing licit and illicit funds)	3.0	3.0	3.0	3.0	LOW
Pass-by (funds are immediately withdrawn or transferred again after transfer)	3.0	3.0	3.0	3.0	LOW

ii. Lending

For fintech lending, the high-risk money laundering (ML) typologies are structuring, smurfing, asset purchases (property, vehicles, crypto assets, etc.), and luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.).

Table 16 High-Risk ML Typologies in Fintech Lending

ML Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Structuring (splitting transactions into smaller amounts conducted repeatedly by one person)	5.95	9.00	9.00	9.00	High
Smurfing (splitting transactions conducted by multiple persons)	5.86	8.67	8.84	8.61	High
Asset purchases (property, vehicles, crypto assets, etc.)	5.87	8.10	8.57	8.03	High
Luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.)	5.82	7.89	8.18	7.54	High
Use of shell companies	3.00	3.00	3.00	3.00	Low
Third-party account control/use of nominees	3.00	3.00	3.00	3.00	Low
Use of stolen or false identity data	3.00	3.00	3.00	3.00	Low
Use of unlicensed service providers	9.00	3.00	3.00	3.00	Low
Transfer to or receipt of funds from high-risk jurisdictions	3.00	3.00	3.00	3.00	Low
Mingling (mixing legitimate and illegitimate funds)	3.00	3.00	3.00	3.00	Low
Pass-by (funds withdrawn or retransferred immediately after transfer)	6.79	3.00	3.00	3.00	Low

iii. Crowdfunding

For fintech crowdfunding, the high-risk money laundering (ML) typologies are structuring, smurfing, asset purchases (property, vehicles, crypto assets, etc.), and luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.).

Table 17 High-Risk ML Typologies in Fintech Crowdfunding

Money Laundering Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Structuring (Breaking transactions into smaller amounts but conducted repeatedly by one person)	9.00	9.00	9.00	9.00	HIGH
Smurfing (Breaking transactions conducted by multiple individuals)	8.86	8.69	8.84	8.61	HIGH
Asset purchases (property, vehicles, etc.)	8.65	7.91	8.39	7.74	HIGH
Luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.)	8.59	7.62	8.02	7.26	HIGH
Use of shell companies	3.00	3.00	3.00	3.00	LOW
Control of third-party accounts / use of nominees	3.00	3.00	3.00	3.00	LOW
Use of false or stolen identity data	3.00	3.00	3.00	3.00	LOW
Use of unlicensed service providers	3.00	3.00	3.00	3.00	LOW
Sending or receiving funds from high-risk jurisdictions	3.00	3.00	3.00	3.00	LOW
Mingling (mixing legitimate and illegitimate funds)	3.00	3.00	3.00	3.00	LOW
Pass-by (funds are immediately withdrawn or transferred again after receipt)	3.00	3.00	3.00	3.00	LOW

iv. Investment

For fintech investment, the high-risk money laundering (ML) typologies include structuring, smurfing, asset purchases (property, vehicles, crypto assets, etc.), mingling (the mixing of legitimate and illicit funds), and the purchase of luxury goods (jewelry, gold, luxury bags, luxury vehicles, etc.).

Table 18. High-Risk ML Typologies in Fintech Investment

ML Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Structuring (breaking transactions into smaller amounts conducted repeatedly by the same person)	6.00	9.00	6.46	9.00	HIGH
Smurfing (breaking transactions conducted by multiple persons)	5.90	8.56	6.37	8.56	HIGH
Asset purchases (property, vehicles, crypto assets, etc.)	5.88	7.91	6.16	7.93	HIGH
Mingling (mixing legitimate and illicit funds)	9.00	3.00	9.00	7.53	HIGH
Purchase of luxury goods (jewelry, gold, luxury bags, luxury vehicles, etc.)	5.80	7.65	5.91	7.52	HIGH
Control of third-party accounts/use of nominees	3.00	3.00	8.76	4.09	LOW
Use of shell companies	6.79	3.00	3.00	3.71	LOW
Use of unlicensed service providers	6.60	3.00	3.00	3.68	LOW
Pass-by (funds withdrawn in cash or retransferred immediately after transfer)	4.51	3.00	3.00	3.29	LOW
Use of false or stolen identity data	3.00	3.00	3.00	3.00	LOW
Sending or receiving funds from high-risk jurisdictions	3.00	3.00	3.00	3.00	LOW

d. Terrorist Financing Typologies

For terrorist financing (TF), based on respondents' perceptions, the high-risk typologies include the use of funds for domestic terrorist operations involving forged identity documents and the collection of funds through legal channels.

Table 19. High-Risk TF Typologies in Fintech

TF Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
1. Fund Raising					
1.a Legal					
Terrorist Sponsor/Fundraiser	8.63	9.00	7.90	8.29	HIGH
Legal Donation Collection	8.67	8.83	7.77	8.19	HIGH
Crowdfunding Funding	8.19	8.81	7.88	8.09	HIGH
Business-to-Business (B2B) Business	8.29	7.88	7.51	7.69	HIGH
Self-Funding (outside business activities)	8.22	8.43	7.60	7.85	HIGH
1.b Illegal					
Extortion	3.35	3.29	3.02	3.09	LOW
Kidnapping for Ransom	3.25	3.00	3.00	3.00	LOW
Exploitation of Natural Resources	3.00	3.64	3.33	3.20	LOW
Other Criminal Activities	3.75	3.56	3.42	3.48	LOW
2. Fund Transfer	5.98	4.96	4.56	4.81	LOW
3. Use of Fund					
3a. Domestic Terrorist Operations					
Forged Identity Documents	9.00	8.82	9.00	9.00	HIGH
Travel to terrorist locations	5.59	5.71	5.27	5.21	MEDIUM
Purchase and maintenance of vehicles or machinery	4.92	5.21	3.60	4.12	LOW
Purchase of weapons and explosives	6.02	5.19	4.57	4.87	LOW
Daily operational expenses	6.39	5.76	5.52	5.57	MEDIUM
Wages for fighters	6.24	5.69	5.29	5.40	MEDIUM
3b. Propaganda and Recruitment					

Social media content	5.28	3.67	4.56	4.35	LOW
Website creation and maintenance	4.48	3.80	4.06	3.94	LOW
Other media production	5.21	4.15	4.30	4.34	LOW
3c. Training					
Ideology	4.67	3.90	3.76	3.87	LOW
Training camp development	4.92	4.73	3.71	4.08	LOW
Communication and translation	5.28	4.43	4.10	4.29	LOW
3d. Overseas Terrorist Operations					
Travel costs for foreign terrorist fighters	6.56	6.01	4.75	5.29	MEDIUM

Table 20. High-Risk TF Typologies in Fintech Payment and Remittance

TF Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
1. Fundraising					
1.a Legal					
Sponsor Funding (Terrorist Financier/Fundraiser)	8.35	8.46	7.92	8.08	HIGH
Fundraising via Donation through NGOs	8.21	8.59	7.78	8.04	HIGH
Crowdfunding-based Funding	8.03	8.83	7.86	7.92	HIGH
Business-based Funding	7.87	8.15	7.51	7.64	HIGH
Self-Funding (other than business income)	7.87	7.83	7.53	7.51	HIGH
1b.Illegal					
Extortion	5.97	5.04	4.91	4.89	LOW
Kidnapping for Ransom	3.81	3.65	3.29	3.41	LOW
Exploitation of Natural Resources Illegally	3.00	3.57	3.17	3.20	LOW
Other Criminal Proceeds	3.38	3.31	3.12	3.16	LOW
2. Fund Transfer	3.25	3.00	3.00	3.00	LOW
3. Use of Fund					
3.a Domestic Terrorist Operations					
Fake Identity Documents	9.00	9.00	9.00	9.00	HIGH
Living Expenses	6.33	5.63	5.79	5.53	MEDIUM

Courier/Delivery Costs	6.15	5.51	5.52	5.34	MEDIUM
Travel to and from Terrorist Locations	5.46	5.45	5.40	5.12	MEDIUM
Purchase of Weapons and Explosives	6.10	5.10	5.00	4.97	LOW
Purchase and Maintenance of Vehicles	4.67	4.53	3.76	4.04	LOW
3b. Propaganda and Recruitment					
Social Media Account Creation and Maintenance	5.10	4.18	4.48	4.24	LOW
Website Creation and Maintenance	4.90	4.06	4.44	4.14	LOW
Other Promotional Media	4.48	3.95	4.25	3.96	LOW
3c. Training					
Ideology	4.73	4.62	3.80	4.10	LOW
Construction of Training Locations	4.76	4.42	3.92	4.07	LOW
Communication Facilities	5.11	3.98	4.13	4.05	LOW
Purchase of Weapons and Explosives (Training)	4.74	4.13	3.69	3.89	LOW
3d. Overseas Terrorist Operations					
Travel Costs of Foreign Terrorist Fighters	6.33	5.81	4.74	5.18	MEDIUM

Table 21 High-Risk TF Typologies in Fintech Lending

TF Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
1. Fund Collection					
1.b. Legal					
Sponsor/Fundraiser for Terrorists	9.00	9.00	7.77	8.55	HIGH
Fundraising through Online Donation Platforms	8.51	8.12	7.50	8.00	HIGH
Crowdfunding-Based Funding	7.65	8.56	7.09	7.61	HIGH
Legitimate Business Operations	8.39	8.56	6.55	7.54	HIGH
1b. Illegal					
Extortion	5.69	4.17	3.55	4.15	LOW
Kidnapping and Ransom	3.00	3.88	4.09	3.59	LOW
Illegal Exploitation of Natural Resources	3.49	3.00	4.09	3.53	LOW
Other Criminal Proceeds	3.24	3.00	3.27	3.11	LOW
2. Transfer of Fund	3.24	3.00	3.00	3.00	LOW
3. Use of Fund					

3a. Domestic Terrorist Operations					
Fake Identity Documents	8.63	8.56	9.00	9.00	HIGH
Travel and Accommodation Expenses	5.69	5.93	4.91	5.22	MEDIUM
Living Expenses	6.18	5.63	4.64	5.15	MEDIUM
Travel/Shipping Costs	6.18	5.63	4.64	5.15	MEDIUM
Purchase and Maintenance of Vehicles or Machinery	5.45	6.51	3.27	4.48	LOW
Purchase of Weapons and Explosives	5.45	4.76	3.27	4.09	LOW
3b. Propaganda and Recruitment					
Creation and Maintenance of Social Media Accounts	5.33	3.15	4.50	4.25	LOW
Creation of News Websites or Online Media	4.96	3.29	4.36	4.12	LOW
Website Creation and Maintenance	5.20	3.88	3.82	4.08	LOW
Other Promotional Media	4.22	3.29	3.55	3.56	LOW
3c. Training					
Ideological Training	5.45	5.63	4.09	4.68	LOW
Construction of Training Facilities	5.69	5.05	3.82	4.48	LOW
Communication Facilities	5.20	4.76	3.55	4.15	LOW
Purchase of Weapons and Explosives (Training)	4.22	4.46	3.55	3.82	LOW
Purchase of Weapons and Ammunition	4.22	3.29	4.09	3.78	LOW
3d. Overseas Terrorist Operations					
Travel Expenses for Foreign Terrorist Fighters	7.10	6.56	5.01	5.83	MEDIUM

Table 22 High-Risk TF Typologies in Fintech Crowdfunding

TF Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
1. Fundraising					
a. Legal					
Private Sponsor (Terrorist Financier/Fundraiser)	9.00	8.61	8.58	9.00	HIGH
Donation Collection through CSOs	7.86	9.00	8.50	8.66	HIGH
Crowdfunding Funding	8.46	7.70	8.40	8.42	HIGH
Legitimate Business	8.94	8.50	7.63	8.41	HIGH

Self-Funding (other than legitimate business)	8.66	7.45	8.06	8.22	HIGH
b. Illegal					
Extortion	5.42	4.24	3.73	4.13	LOW
Smuggling with Illegal Levy	3.00	3.99	4.26	3.58	LOW
Illegal Exploitation of Natural Resources	3.44	3.25	4.26	3.52	LOW
Other Criminal Proceeds	3.22	3.25	3.42	3.11	LOW
2. Fund Transfer	3.22	3.25	3.14	3.00	LOW
3. Use of Fund					
3a. Domestic Terrorist Operations					
False Identity Documents	7.84	7.72	9.00	8.52	HIGH
Travel to/from Terrorist Locations	5.53	5.98	5.23	5.32	MEDIUM
Basic Living Expenses	5.97	5.36	4.95	5.15	MEDIUM
Courier Fees	5.86	5.24	4.81	5.02	MEDIUM
Purchase and Maintenance of Vehicles or Machinery	5.31	6.48	3.56	4.58	LOW
Purchase of Weapons and Explosives	5.31	4.61	3.56	4.11	LOW
3b. Propaganda and Recruitment					
Creation and Maintenance of Social Media Accounts	4.87	3.00	4.40	3.94	LOW
Creation and Maintenance of News Sites	4.65	3.25	4.44	3.94	LOW
Website Creation and Maintenance	4.87	3.75	3.84	3.89	LOW
Other Promotional Media	3.99	3.25	3.56	3.39	LOW
3c. Training					
Ideology	8.39	4.24	3.00	4.62	LOW
Training Location Development	5.09	5.24	4.12	4.46	LOW
Communication Facilities / Sanitation	5.31	4.74	3.84	4.27	LOW
Purchase of Weapons and Explosives (Training)	4.87	4.49	3.56	3.95	LOW
Other Training Expenses	3.99	4.24	3.56	3.64	LOW
3d. Overseas Terrorist Operations					
Travel Expenses of Foreign Terrorist Fighters	6.32	6.09	4.95	5.46	MEDIUM

Tabel 23 – High-Risk TF Typologies in Fintech Investment

TF Typology	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
1. Fund Collection					
1.a. Legal					
Sponsor/Funding of Terrorist Financier/Fundraiser	9.00	9.00	8.43	9.00	HIGH
Fundraising Deposits	8.08	9.00	8.14	8.51	HIGH
Donations through Mass Organizations	8.77	9.00	7.57	8.43	HIGH
Crowdfunding Funding	8.31	8.10	7.86	8.18	HIGH
Self-Funding (outside business activities)	8.77	7.80	7.57	8.11	HIGH
1b. Illegal					
Extortion	3.23	3.00	3.00	3.00	LOW
Abduction with Ransom	3.23	3.00	3.29	3.12	LOW
Exploitation of Natural Resources Legally	3.00	3.90	4.14	3.60	LOW
Other Criminal Proceeds	3.46	3.00	4.14	3.53	LOW
2. Fund Transfer	5.54	4.20	3.61	4.19	LOW
3. Use of Fund					
3a. Domestic Terrorist Operations					
False Identity Documents	8.08	8.40	9.00	8.81	HIGH
Travel from and to Terrorist Locations	5.54	5.70	5.00	5.18	MEDIUM
Daily Living Expenses	6.00	5.40	4.71	5.12	MEDIUM
Courier Costs	6.00	5.40	4.71	5.12	MEDIUM
Purchase and Maintenance of Vehicles or Machinery	5.31	6.30	3.29	4.44	LOW
Purchase of Weapons and Explosives	5.31	4.50	3.29	4.04	LOW
3b. Propaganda and Recruitment					
Creation and Maintenance of Social Media Accounts	5.31	3.00	4.71	4.34	LOW
Creation and Maintenance of News Websites	5.08	3.30	4.71	4.34	LOW
Creation and Maintenance of Websites	5.31	3.90	4.14	4.29	LOW
Other Promotional Media	4.38	3.30	3.86	3.76	LOW
3c. Training					
Ideology	5.54	5.40	4.43	4.84	LOW

Construction of Training Facilities	5.77	4.80	4.14	4.64	LOW
Communication of Secrets/Symbols	5.31	4.50	3.86	4.30	LOW
Manufacture of Weapons and Explosives	4.38	4.20	3.86	3.96	LOW
Use of Weapons and Explosives	4.38	3.00	4.43	3.93	LOW
Bait	4.38	4.20	3.29	3.71	LOW
3d. Overseas Terrorist Operations					
Travel Expenses of Foreign Terrorist Fighters	6.68	6.28	5.00	5.68	MEDIUM

e. Region

In general, the region considered to be at high risk for money laundering (ML) is DKI Jakarta. West Java is categorized as a medium-risk region. Most fintech companies are headquartered in DKI Jakarta, and a very large volume of fintech transactions takes place in DKI Jakarta as the center of government and business activities. With regard to terrorist financing (TF), West Java and DKI Jakarta are considered high-risk regions. Court decisions on TF cases involving fintech have originated from West Java.

Table 24 High-Risk Regions for ML in Fintech

Region (ML)	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
DKI Jakarta	9.0	9.0	9.0	9.0	HIGH
West Java	5.85	7.27	6.35	5.8	MEDIUM
East Java	4.16	7.21	5.73	4.97	LOW
Central Java	3.82	5.82	4.05	3.88	LOW
Bali	3.67	5.7	4.02	3.82	LOW
North Sumatra	3.73	4.93	4.0	3.74	LOW
North Sulawesi	4.29	4.03	3.93	3.72	LOW
Riau	3.47	5.48	3.88	3.69	LOW
Papua	3.42	5.58	3.84	3.68	LOW
Lampung	3.54	4.72	3.92	3.64	LOW
Banten	3.61	4.73	3.83	3.62	LOW
Riau Islands	3.42	4.83	3.82	3.59	LOW
South Sumatra	3.58	4.51	3.8	3.58	LOW
West Kalimantan	3.33	4.39	3.74	3.49	LOW
West Papua	3.38	5.35	3.36	3.43	LOW
South Sulawesi	3.29	3.59	3.64	3.36	LOW
West Sumatra	3.23	3.59	3.66	3.35	LOW
DI Yogyakarta	3.38	4.55	3.35	3.35	LOW
Aceh	3.32	4.59	3.29	3.32	LOW
East Kalimantan	3.39	4.31	3.27	3.29	LOW
South Kalimantan	3.3	4.3	3.29	3.29	LOW
North Kalimantan	3.2	4.25	3.19	3.22	LOW
Central Kalimantan	3.24	4.11	3.19	3.22	LOW
Maluku	3.15	4.02	3.19	3.19	LOW
West Nusa Tenggara	3.18	3.83	3.2	3.18	LOW
North Maluku	3.17	3.93	3.1	3.15	LOW
Bengkulu	3.18	3.68	3.15	3.15	LOW
East Nusa Tenggara	3.1	3.74	3.13	3.14	LOW
Jambi	3.13	3.59	3.13	3.12	LOW
Southeast Sulawesi	3.15	3.52	3.06	3.1	LOW
Gorontalo	3.09	3.51	3.09	3.09	LOW
Central Sulawesi	3.12	3.36	3.06	3.08	LOW
West Sulawesi	3.09	3.36	3.03	3.06	LOW
Bangka Belitung Islands	3.0	3.0	3.0	3.0	LOW

Table 25 High-Risk Regions for TF in Fintech

TF Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
West Java	9.0	7.13	9.0	9.0	HIGH
DKI Jakarta	8.33	9.0	7.72	8.18	HIGH
East Java	4.12	7.56	3.99	4.22	LOW
Central Java	3.88	6.26	4.2	4.11	LOW
Papua	3.73	7.05	3.74	3.93	LOW
North Sumatra	3.69	5.63	3.66	3.72	LOW
West Papua	3.55	5.97	3.53	3.66	LOW
Bali	3.58	5.51	3.59	3.65	LOW
Lampung	3.55	5.59	3.58	3.65	LOW
Aceh	3.54	5.83	3.51	3.63	LOW
Banten	3.43	5.2	3.49	3.53	LOW
Special Region of Yogyakarta	3.45	5.06	3.47	3.51	LOW
South Sumatra	3.49	4.9	3.43	3.48	LOW
Riau	3.33	4.74	3.45	3.44	LOW
Riau Islands	3.34	4.52	3.37	3.38	LOW
West Sumatra	3.39	4.4	3.34	3.37	LOW
South Kalimantan	3.32	4.46	3.31	3.34	LOW
East Kalimantan	3.32	4.47	3.3	3.34	LOW
West Nusa Tenggara	3.27	4.29	3.31	3.32	LOW
Central Kalimantan	3.27	4.25	3.25	3.29	LOW
Maluku	3.21	4.22	3.28	3.29	LOW
West Kalimantan	3.29	3.98	3.27	3.27	LOW
South Sulawesi	3.3	3.84	3.24	3.25	LOW
North Kalimantan	3.2	4.17	3.18	3.24	LOW
Central Sulawesi	3.22	4.05	3.16	3.22	LOW
Bengkulu	3.17	3.81	3.18	3.19	LOW
North Sulawesi	3.21	3.75	3.16	3.19	LOW
East Nusa Tenggara	3.13	3.88	3.17	3.19	LOW
North Maluku	3.18	3.73	3.11	3.15	LOW
Gorontalo	3.11	3.57	3.14	3.14	LOW
Southeast Sulawesi	3.18	3.55	3.11	3.14	LOW
Jambi	3.11	3.42	3.14	3.12	LOW
West Sulawesi	3.17	3.25	3.08	3.09	LOW
Bangka Belitung Islands	3.0	3.0	3.0	3.0	LOW

i. Payments and Remittances

For fintech payment and remittance services, the region assessed as having a high risk of money laundering (ML) is DKI Jakarta. Meanwhile, the region assessed as having a high risk of terrorist financing (TF) is West Java.

Table 26 High-Risk Regions for ML in Fintech Payment and Remittance Services

ML Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
DKI Jakarta	9.0	9.0	9.0	9.0	HIGH
West Java	6.28	7.34	7.55	6.64	MEDIUM
East Java	5.74	7.15	7.44	6.36	MEDIUM
North Sumatra	5.51	4.82	7.14	5.52	MEDIUM
Central Java	4.85	5.65	6.53	5.25	MEDIUM
Lampung	4.85	4.83	6.95	5.24	MEDIUM
Bali	4.11	5.73	6.71	5.14	MEDIUM
Banten	4.77	4.63	6.52	4.98	MEDIUM
South Sumatra	4.66	4.45	6.64	4.96	MEDIUM
Riau	3.96	5.45	6.3	4.86	MEDIUM
Papua	3.42	5.59	6.38	4.78	LOW
Riau Islands	3.41	4.86	6.15	4.51	LOW
South Sulawesi	3.99	3.54	6.55	4.51	LOW
West Kalimantan	3.31	4.45	6.38	4.48	LOW
West Sumatra	3.22	3.58	6.59	4.32	LOW
West Papua	3.38	5.4	3.38	3.52	LOW
Aceh	3.32	4.57	3.29	3.36	LOW
DI Yogyakarta	3.33	4.45	3.29	3.35	LOW
East Kalimantan	3.38	4.32	3.24	3.32	LOW
South Kalimantan	3.27	4.31	3.27	3.31	LOW
North Kalimantan	3.21	4.29	3.22	3.28	LOW
Central Kalimantan	3.24	4.13	3.2	3.26	LOW
Maluku	3.16	4.09	3.2	3.24	LOW
North Sulawesi	3.25	3.93	3.16	3.22	LOW
West Nusa Tenggara	3.16	3.92	3.19	3.21	LOW
North Maluku	3.16	3.96	3.1	3.19	LOW
East Nusa Tenggara	3.11	3.8	3.14	3.17	LOW
Bengkulu	3.14	3.68	3.1	3.14	LOW
Jambi	3.1	3.54	3.1	3.12	LOW
Southeast Sulawesi	3.14	3.52	3.06	3.11	LOW
Gorontalo	3.09	3.49	3.09	3.11	LOW
Central Sulawesi	3.11	3.35	3.06	3.08	LOW
West Sulawesi	3.09	3.35	3.05	3.08	LOW
Bangka Belitung Islands	3.0	3.0	3.0	3.0	LOW

Table 27 High-Risk Regions for TF in Fintech Payment and Remittance

TF Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
West Java	9.00	7.11	9.00	9.00	HIGH
DKI Jakarta	6.77	9.00	6.04	6.71	MEDIUM
East Java	4.15	7.68	4.00	4.48	LOW
Central Java	3.95	6.14	4.67	4.47	LOW
Papua	3.75	7.22	3.82	4.21	LOW
West Papua	3.58	6.10	3.59	3.86	LOW
Aceh	3.59	6.16	3.56	3.86	LOW
North Sumatra	3.70	5.62	3.67	3.84	LOW
Lampung	3.55	5.70	3.60	3.79	LOW
Bali	3.59	5.49	3.57	3.74	LOW
Banten	3.47	5.35	3.50	3.66	LOW
DI Yogyakarta	3.47	5.13	3.46	3.61	LOW
South Sumatra	3.52	4.94	3.43	3.58	LOW
Riau	3.31	4.58	3.45	3.49	LOW
West Sumatra	3.38	4.52	3.38	3.46	LOW
Riau Islands	3.35	4.54	3.34	3.44	LOW
East Kalimantan	3.33	4.51	3.28	3.41	LOW
South Kalimantan	3.33	4.50	3.29	3.41	LOW
West Nusa Tenggara	3.27	4.43	3.33	3.40	LOW
Central Kalimantan	3.30	4.31	3.27	3.36	LOW
Maluku	3.23	4.29	3.30	3.36	LOW
North Kalimantan	3.21	4.22	3.22	3.31	LOW
West Kalimantan	3.30	3.97	3.26	3.30	LOW
Central Sulawesi	3.18	4.12	3.17	3.27	LOW
East Nusa Tenggara	3.15	4.00	3.19	3.25	LOW
South Sulawesi	3.31	3.71	3.22	3.25	LOW
Bengkulu	3.18	3.76	3.15	3.20	LOW
North Sulawesi	3.21	3.69	3.15	3.20	LOW
North Maluku	3.18	3.66	3.11	3.18	LOW
Southeast Sulawesi	3.18	3.51	3.12	3.16	LOW
Gorontalo	3.12	3.50	3.15	3.15	LOW
Jambi	3.11	3.34	3.12	3.12	LOW
West Sulawesi	3.18	3.17	3.11	3.10	LOW
Bangka Belitung Islands	3.00	3.00	3.00	3.00	LOW

ii. Lending

For fintech lending, the regions considered to have a high ML risk are DKI Jakarta, East Java, and West Java. Meanwhile, the region considered to have a high TF risk is West Java.

Table 28 High-Risk ML Regions for Fintech Lending

ML Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
DKI Jakarta	9.00	9.00	9.00	9.00	HIGH
East Java	7.92	7.33	8.13	7.65	HIGH
West Java	8.04	7.12	8.13	7.63	HIGH
Central Java	6.96	6.21	7.07	6.47	MEDIUM
Bali	6.24	5.65	6.53	5.85	MEDIUM
North Sumatra	6.00	5.16	6.13	5.47	MEDIUM
Banten	5.82	4.95	6.13	5.37	MEDIUM
DI Yogyakarta	5.22	4.81	5.47	4.87	LOW
Papua	4.98	5.65	5.13	4.84	LOW
Riau	4.68	5.51	5.27	4.79	LOW
Riau Islands	4.86	4.81	5.40	4.74	LOW
South Sumatra	5.22	4.67	5.20	4.72	LOW
Lampung	4.86	4.60	5.33	4.67	LOW
West Papua	4.68	5.57	4.67	4.49	LOW
West Kalimantan	4.86	4.26	4.80	4.36	LOW
East Kalimantan	4.68	4.26	4.80	4.31	LOW
South Kalimantan	4.56	4.26	4.73	4.26	LOW
Aceh	4.44	4.60	4.53	4.21	LOW
South Sulawesi	4.44	3.70	4.40	3.97	LOW
Bengkulu	4.32	3.70	4.40	3.94	LOW
North Sulawesi	4.08	4.19	3.93	3.79	LOW
West Nusa Tenggara	4.02	3.70	4.20	3.79	LOW
Central Kalimantan	4.02	4.05	3.87	3.72	LOW
West Sumatra	4.14	3.84	3.87	3.71	LOW
Jambi	3.84	3.70	4.07	3.70	LOW
Maluku	3.54	3.98	3.93	3.63	LOW
North Kalimantan	3.72	4.19	3.60	3.58	LOW
North Maluku	3.78	3.98	3.60	3.55	LOW
East Nusa Tenggara	3.42	3.70	3.60	3.42	LOW
West Sulawesi	3.36	3.42	3.30	3.33	LOW
Southeast Sulawesi	3.36	3.56	3.40	3.33	LOW
Gorontalo	3.36	3.56	3.40	3.33	LOW
Bangka Belitung Islands	3.00	3.00	3.00	3.00	LOW

Table 29 High-Risk TF Regions for Fintech Lending

TF Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
West Java	9.00	7.11	9.00	9.00	HIGH
DKI Jakarta	6.77	9.00	6.04	6.71	MEDIUM
East Java	4.15	7.68	4.00	4.48	LOW
Central Java	3.95	6.14	4.67	4.47	LOW
Papua	3.75	7.22	3.82	4.21	LOW
West Papua	3.58	6.10	3.59	3.86	LOW
Aceh	3.59	6.16	3.56	3.86	LOW
North Sumatra	3.70	5.62	3.67	3.84	LOW
Lampung	3.55	5.70	3.60	3.79	LOW
Bali	3.59	5.49	3.57	3.74	LOW
Banten	3.47	5.35	3.50	3.66	LOW
DI Yogyakarta	3.47	5.13	3.46	3.61	LOW
South Sumatra	3.52	4.94	3.43	3.58	LOW
Riau	3.31	4.58	3.45	3.49	LOW
West Sumatra	3.38	4.52	3.38	3.46	LOW
Riau Islands	3.35	4.54	3.34	3.44	LOW
East Kalimantan	3.33	4.51	3.28	3.41	LOW
South Kalimantan	3.33	4.50	3.29	3.41	LOW
West Nusa Tenggara	3.27	4.43	3.33	3.40	LOW
Central Kalimantan	3.30	4.31	3.27	3.36	LOW
Maluku	3.23	4.29	3.30	3.36	LOW
North Kalimantan	3.21	4.22	3.22	3.31	LOW
West Kalimantan	3.30	3.97	3.26	3.30	LOW
Central Sulawesi	3.18	4.12	3.17	3.27	LOW
East Nusa Tenggara	3.15	4.00	3.19	3.25	LOW
South Sulawesi	3.31	3.71	3.22	3.25	LOW
Bengkulu	3.18	3.76	3.15	3.20	LOW
North Maluku	3.18	3.66	3.11	3.18	LOW
Southeast Sulawesi	3.18	3.51	3.12	3.16	LOW
Gorontalo	3.12	3.50	3.15	3.15	LOW
Jambi	3.11	3.34	3.12	3.12	LOW
West Sulawesi	3.18	3.17	3.11	3.10	LOW
Bangka Belitung Islands	3.00	3.00	3.00	3.00	LOW

iii. Crowdfunding

For fintech crowdfunding, the regions assessed as having a high ML risk are DKI Jakarta and East Java. Meanwhile, the regions assessed as having a high TF risk are DKI Jakarta, West Java, and East Java.

Table 30 High-Risk ML Regions for Fintech Crowdfunding

ML Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
DKI Jakarta	9.0	9.0	9.0	9.0	HIGH
East Java	8.08	7.34	8.2	7.74	HIGH
West Java	8.2	7.12	8.2	7.72	HIGH
Central Java	7.1	6.25	7.07	6.51	MEDIUM
Bali	6.37	5.67	6.53	5.88	MEDIUM
North Sumatra	6.12	5.17	6.27	5.55	MEDIUM
Banten	5.76	4.95	6.13	5.34	MEDIUM
DI Yogyakarta	5.27	4.81	5.47	4.86	MEDIUM
Papua	5.08	5.67	5.13	4.84	LOW
Riau Islands	4.96	4.88	5.47	4.79	LOW
Riau	4.71	5.53	5.27	4.78	LOW
South Sumatra	5.33	4.66	5.2	4.72	LOW
Lampung	5.02	4.59	5.33	4.69	LOW
West Papua	4.78	5.39	4.67	4.49	LOW
East Kalimantan	4.9	4.3	4.87	4.38	LOW
West Kalimantan	4.78	4.3	4.87	4.35	LOW
South Kalimantan	4.65	4.3	4.8	4.3	LOW
Aceh	4.47	4.59	4.53	4.19	LOW
South Sulawesi	4.47	3.65	4.4	3.95	LOW
Bengkulu	4.35	3.65	4.4	3.92	LOW
North Sulawesi	4.1	4.16	3.93	3.76	LOW
West Nusa Tenggara	4.04	3.65	4.2	3.76	LOW
Central Kalimantan	4.04	4.08	3.93	3.74	LOW
West Sumatra	4.16	3.8	3.87	3.68	LOW
Jambi	3.86	3.65	4.07	3.67	LOW
Maluku	3.61	3.94	3.93	3.61	LOW
North Kalimantan	3.73	4.23	3.67	3.59	LOW
North Maluku	3.86	3.94	3.6	3.53	LOW
East Nusa Tenggara	3.43	3.65	3.6	3.39	LOW
Southeast Sulawesi	3.8	3.51	3.4	3.36	LOW
Gorontalo	3.43	3.58	3.53	3.35	LOW
Central Sulawesi	3.67	3.36	3.4	3.31	LOW
West Sulawesi	3.37	3.36	3.0	3.09	LOW
Bangka Belitung Islands	3.0	3.0	3.13	3.0	LOW

Table 31 High-Risk TF Regions for Fintech Crowdfunding

TF Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
DKI Jakarta	9.00	9.00	9.00	9.00	HIGH
West Java	7.74	7.20	7.85	7.41	HIGH
East Java	7.67	7.29	7.85	7.41	HIGH
Central Java	6.98	6.60	7.08	6.60	MEDIUM
North Sumatra	6.07	5.66	6.31	5.71	MEDIUM
Papua	6.07	6.77	5.77	5.69	MEDIUM
Bali	5.58	5.74	6.31	5.59	MEDIUM
Lampung	5.51	5.49	5.85	5.29	MEDIUM
DI Yogyakarta	4.81	5.06	5.54	4.86	LOW
West Papua	5.09	5.91	4.92	4.83	LOW
South Sumatra	4.88	4.89	5.23	4.71	LOW
Riau	4.67	5.23	5.15	4.69	LOW
Banten	4.40	4.71	5.38	4.61	LOW
Riau Islands	4.40	4.54	5.46	4.61	LOW
Aceh	4.60	5.06	4.92	4.53	LOW
South Kalimantan	4.33	4.37	5.00	4.35	LOW
East Kalimantan	4.40	4.37	4.77	4.27	LOW
West Sumatra	4.88	4.37	4.31	4.19	LOW
West Kalimantan	4.19	4.03	4.77	4.15	LOW
South Sulawesi	4.26	4.20	4.62	4.13	LOW
West Nusa Tenggara	4.19	4.03	4.54	4.05	LOW
Bengkulu	3.70	4.03	4.62	3.96	LOW
North Sulawesi	3.98	3.94	4.23	3.85	LOW
Central Kalimantan	4.05	4.11	4.00	3.80	LOW
Central Sulawesi	4.47	4.03	3.77	3.79	LOW
Maluku	3.70	4.20	4.08	3.77	LOW
Jambi	3.42	3.69	4.08	3.61	LOW
North Kalimantan	3.77	4.11	3.54	3.55	LOW
North Maluku	3.77	4.03	3.54	3.53	LOW
Gorontalo	3.42	3.86	3.69	3.49	LOW
West Nusa Tenggara	3.91	3.69	3.46	3.47	LOW
East Nusa Tenggara	3.35	3.69	3.69	3.44	LOW
West Sulawesi	3.56	3.51	3.00	3.18	LOW
Bangka Belitung Islands	3.00	3.00	3.08	3.00	LOW

iv. Investment

For fintech investment, the region with a high risk of money laundering (ML) is DKI Jakarta. Meanwhile, the region with a high risk of terrorist financing (TF) is West Java.

Table 32 High-Risk ML Regions for Investment Fintech

ML Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
DKI Jakarta	9.00	9.00	9.00	9.00	HIGH
West Java	6.47	7.29	6.79	6.25	MEDIUM
East Java	5.67	7.43	5.98	5.56	MEDIUM
Central Java	3.91	6.29	3.85	3.87	LOW
Bali	3.74	5.71	3.74	3.72	LOW
North Sumatra	3.72	5.14	3.65	3.61	LOW
Banten	3.63	4.86	3.62	3.55	LOW
Papua	3.47	5.71	3.42	3.52	LOW
Riau	3.36	5.57	3.48	3.51	LOW
DI Yogyakarta	3.52	4.86	3.51	3.48	LOW
Riau Islands	3.47	4.86	3.48	3.46	LOW
West Papua	3.39	5.43	3.34	3.44	LOW
South Sumatra	3.50	4.71	3.45	3.44	LOW
Lampung	3.41	4.57	3.48	3.42	LOW
Aceh	3.34	4.64	3.31	3.34	LOW
East Kalimantan	3.41	4.29	3.37	3.34	LOW
West Kalimantan	3.39	4.29	3.37	3.34	LOW
South Kalimantan	3.36	4.29	3.37	3.33	LOW
South Sulawesi	3.33	3.71	3.31	3.25	LOW
North Sulawesi	3.25	4.29	3.20	3.24	LOW
Bengkulu	3.33	3.71	3.28	3.23	LOW
Central Kalimantan	3.25	4.14	3.17	3.22	LOW
Maluku	3.17	4.00	3.20	3.20	LOW
West Nusa Tenggara	3.22	3.71	3.23	3.19	LOW
West Sumatra	3.25	3.86	3.17	3.19	LOW
Jambi	3.22	3.71	3.20	3.18	LOW
North Kalimantan	3.17	4.14	3.11	3.18	LOW
North Maluku	3.19	4.00	3.11	3.17	LOW
East Nusa Tenggara	3.11	3.71	3.11	3.13	LOW
Southeast Sulawesi	3.17	3.57	3.08	3.11	LOW
Gorontalo	3.11	3.57	3.08	3.11	LOW
Central Sulawesi	3.14	3.43	3.08	3.10	LOW
West Sulawesi	3.08	3.43	3.00	3.05	LOW
Bangka Belitung Islands	3.00	3.00	3.00	3.00	LOW

Table 33 High-Risk Regions for TF Risk in Fintech

TF Risk Region	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
West Java	9.0	7.33	9.0	9.0	HIGH
DKI Jakarta	4.39	9.0	4.3	4.64	LOW
East Java	4.04	7.33	3.94	4.14	LOW
Central Java	3.88	6.5	3.78	3.92	LOW
Papua	3.69	6.67	3.62	3.82	LOW
North Sumatra	3.66	5.67	3.62	3.69	LOW
Bali	3.57	5.67	3.58	3.66	LOW
Lampung	3.54	5.33	3.55	3.6	LOW
West Papua	3.47	5.83	3.42	3.58	LOW
Riau	3.38	5.17	3.45	3.5	LOW
DI Yogyakarta	3.41	5.0	3.45	3.49	LOW
Aceh	3.41	5.17	3.39	3.48	LOW
South Sumatra	3.41	4.83	3.36	3.43	LOW
Riau Islands	3.35	4.5	3.39	3.39	LOW
Banten	3.32	4.67	3.32	3.37	LOW
West Sumatra	3.44	4.33	3.29	3.35	LOW
South Kalimantan	3.28	4.33	3.32	3.33	LOW
East Kalimantan	3.28	4.33	3.26	3.3	LOW
North Sulawesi	3.28	4.17	3.26	3.28	LOW
Maluku	3.19	4.17	3.26	3.27	LOW
West Kalimantan	3.25	4.0	3.26	3.26	LOW
West Nusa Tenggara	3.25	4.0	3.23	3.25	LOW
Central Kalimantan	3.22	4.17	3.19	3.24	LOW
Central Sulawesi	3.32	4.0	3.19	3.24	LOW
North Sulawesi	3.22	4.0	3.16	3.21	LOW
Bengkulu	3.16	4.0	3.16	3.2	LOW
North Kalimantan	3.16	4.0	3.13	3.19	LOW
Maluku Utara	3.19	4.0	3.1	3.18	LOW
Gorontalo	3.13	3.83	3.13	3.16	LOW
Southeast Sulawesi	3.19	3.67	3.1	3.14	LOW
East Nusa Tenggara	3.09	3.67	3.13	3.14	LOW
Jambi	3.13	3.67	3.1	3.13	LOW
West Sulawesi	3.13	3.5	3.03	3.09	LOW
Bangka Belitung Islands	3.0	3.0	3.0	3.0	LOW

f. Profile

In general, the profiles considered to be at high risk of money laundering (ML) are entrepreneurs/self-employed individuals, while the profiles considered to be at high risk of terrorist financing (TF) are traders and entrepreneurs/self-employed individuals.

Table 34 High-Risk Profiles for ML in Fintech

ML Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Entrepreneurs/Self-employed Individuals	9.00	8.61	9.00	9.00	HIGH
Legislative and Government Officials	4.57	9.00	4.52	4.76	LOW
Civil Servants (including retirees)	4.60	8.36	4.45	4.64	LOW
Indonesian National Armed Forces / National Police (including retirees)	4.49	8.34	4.44	4.61	LOW
Employees of SOEs/RSOEs (including retirees)	4.42	7.39	4.25	4.36	LOW
Money Changer Employees	4.87	5.55	4.55	4.35	LOW
Parole Officers	4.14	8.76	3.92	4.31	LOW
Private Sector Employees	4.35	6.88	4.18	4.24	LOW
Laborers, Domestic Helpers, Construction Workers	4.26	4.61	4.86	4.21	LOW
Housewives	4.23	6.03	3.97	4.00	LOW
Professionals and Consultants	4.05	5.96	3.87	3.90	LOW
Retirees (Gov/SOEs/RSOEs)	3.65	6.57	3.86	3.89	LOW
NGO/Non-profit Employees	3.83	6.97	3.61	3.86	LOW
Bank Employees	3.83	6.18	3.77	3.84	LOW
Students	3.93	4.33	3.56	3.54	LOW
Traders	3.74	4.31	3.46	3.45	LOW
Teachers and Lecturers	3.66	4.21	3.47	3.43	LOW
Religious/Community Leaders	3.33	4.44	3.44	3.38	LOW
Others	3.61	3.00	3.33	3.22	LOW
Farmers and Fishermen	3.44	3.09	3.21	3.16	LOW
Craftsmen/Artisans	3.00	3.06	3.00	3.00	LOW

Table 35 High-Risk Profiles for TF in Fintech

TF Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Traders	9.00	5.30	9.00	9.00	HIGH
Entrepreneurs/Self-employed	7.32	9.00	7.58	7.97	HIGH
Private Employees	6.73	6.99	6.73	6.75	MEDIUM
Students/University Students	6.88	5.76	6.61	6.50	MEDIUM
Others	6.43	3.12	7.56	6.45	MEDIUM
State-Owned Enterprise Employees (including retirees)	3.57	6.48	4.92	4.51	LOW
Clerics/Religious Leaders and Religious Organizations	3.73	8.39	4.11	4.33	LOW
Managers/Employees of NGOs or Other Non-Legal Entities	3.83	8.21	3.99	4.26	LOW
Correctional Officers (Parole Officers)	3.80	7.74	3.95	4.17	LOW
Military/Police (including retirees)	3.75	7.67	3.96	4.16	LOW
Legislative and Government Officials	3.78	7.41	3.91	4.11	LOW
Employees of Foundations or Other Legal Entities	3.70	7.74	3.85	4.09	LOW
Lecturers and Teachers	3.34	5.73	4.18	3.95	LOW
Civil Servants (including retirees)	3.55	6.70	3.76	3.88	LOW
Professionals and Consultants	3.33	5.34	3.46	3.52	LOW
Bank Employees	3.32	5.13	3.49	3.52	LOW
Homemakers	3.27	4.85	3.46	3.46	LOW
Money Changer Employees	3.26	4.61	3.43	3.41	LOW
Laborers, Domestic Helpers, and Security Personnel	3.00	3.50	3.20	3.13	LOW
Farmers and Fishermen	3.02	3.42	3.12	3.09	LOW
Artisans	3.04	3.00	3.00	3.00	LOW

i. Payments and Remittances

The profiles with a high risk of ML in fintech payments and remittances are entrepreneurs/self-employed individuals, private-sector employees, housewives, and civil servants (including retirees). Meanwhile, the profiles with a high risk of TF are private-sector employees and students.

Table 36 High-Risk ML Profiles for Fintech Payments and Remittances

ML Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Entrepreneurs/Self-employed	7.82	8.60	9.00	9.00	HIGH
Private-sector employees	9.00	6.82	8.78	8.63	HIGH
Housewives	7.22	6.35	8.61	7.68	HIGH
Civil servants (including retirees)	4.67	8.33	8.22	7.21	HIGH
Legislative and government officials	4.24	8.91	7.37	6.74	MEDIUM
SOE employees (including retirees)	3.98	7.55	7.36	6.23	MEDIUM
Students	5.20	4.54	8.35	6.16	MEDIUM
Professionals and consultants	4.04	6.20	7.59	5.93	MEDIUM
Traders	4.40	4.32	7.79	5.54	MEDIUM
Laborers, domestic helpers, and security staff	4.06	4.71	7.59	5.47	MEDIUM
Lecturers and teachers	3.88	4.21	7.27	5.11	MEDIUM
Others	4.25	3.00	7.63	5.00	MEDIUM
Parole officers	4.29	9.00	4.35	4.92	LOW
Farmers and fishermen	4.02	3.01	7.47	4.86	LOW
Military/Police (including retirees)	4.15	8.66	4.30	4.79	LOW
NGO managers/employees (non-incorporated)	3.97	7.28	4.04	4.34	LOW
Foundation/association managers and employees	3.76	7.00	3.88	4.16	LOW
Bank employees	3.66	6.26	3.79	3.97	LOW
Money changer employees	3.54	5.76	3.72	3.82	LOW
Religious leaders	3.28	4.53	3.37	3.41	LOW
Artisans	3.00	3.08	3.00	3.00	LOW

Table 37 High-Risk Terrorist TF Profiles in Fintech Payments and Remittances

TF Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Private-Sector Employee	8.60	6.77	9.00	9.00	HIGH
Student	9.00	5.80	9.00	8.77	HIGH
Trader	7.02	5.42	7.20	6.70	MEDIUM
Entrepreneur / Self-Employed	5.58	9.00	5.74	6.33	MEDIUM
State-Owned Enterprise Employee (including retirees)	3.54	6.17	5.58	4.92	LOW
Religious Leader / Religious Organization Leader	3.73	8.78	4.13	4.75	LOW
Manager / Employee of NGO or Other Unincorporated Organization	3.84	8.47	3.97	4.62	LOW
Military / Police (including retirees)	3.77	7.90	3.95	4.48	LOW
Parole Officer	3.81	7.84	3.94	4.47	LOW
Manager and Employee of Incorporated Foundation/Organization	3.71	8.13	3.86	4.45	LOW
Legislative and Government Official	3.75	7.08	3.87	4.27	LOW
Teacher and Lecturer	3.33	5.55	4.51	4.19	LOW
Civil Servant (including retirees)	3.52	6.59	3.71	4.04	LOW
Professional and Consultant	3.32	5.17	3.43	3.60	LOW
Housewife	3.27	4.95	3.43	3.55	LOW
Others	3.05	3.09	4.40	3.54	LOW
Bank Employee	3.30	4.74	3.45	3.52	LOW
Money Changer Employee	3.25	4.46	3.41	3.45	LOW
Laborer, Domestic Helper, and Security Personnel	3.00	3.46	3.18	3.13	LOW
Farmer and Fisherman	3.04	3.27	3.11	3.08	LOW
Craftsman	3.09	3.00	3.00	3.00	LOW

ii. Lending

In general, the profiles with a high ML risk in fintech lending are private-sector employees and entrepreneurs/self-employed individuals, while the profiles with a high TF risk are traders and others.

Table 38 High-Risk ML Profiles in Fintech Lending

ML Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Private-sector employees	9.00	6.66	8.81	9.0	HIGH
Entrepreneurs/Self-employed	5.96	8.18	9.0	8.25	HIGH
Students	4.99	3.82	8.49	6.26	MEDIUM
Legislative and Government Officials	4.42	9.0	4.51	4.95	LOW
Civil servants (including retirees)	4.22	8.31	4.38	4.7	LOW
Political party officials	4.14	7.86	4.21	4.51	LOW
TNI/Police (including retirees)	4.08	7.55	4.19	4.44	LOW
SOE employees (including retirees)	3.88	6.85	3.97	4.16	LOW
NGO officials/employees and other non-legal-entity organizations	3.73	6.16	3.93	3.99	LOW
Bank employees	3.64	5.97	3.78	3.87	LOW
NGO officials and employees of other legal-entity organizations	3.58	5.78	3.67	3.77	LOW
Homemakers	3.57	5.34	3.72	3.73	LOW
Professionals and consultants	3.51	5.21	3.6	3.64	LOW
Money changer employees	3.5	4.96	3.58	3.59	LOW
Laborers, domestic helpers, and security personnel	3.34	4.52	3.49	3.45	LOW
Traders	3.33	4.39	3.3	3.35	LOW
Religious leaders	3.24	4.27	3.35	3.34	LOW
Lecturers and teachers	3.24	4.08	3.38	3.32	LOW
Others	3.12	3.0	3.24	3.1	LOW
Farmers and fishermen	3.0	3.13	3.09	3.03	LOW
Artisans	3.03	3.13	3.0	3.0	LOW

Table 39 High-Risk TF Profiles – Fintech Lending

TF Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Traders	9.00	5.25	9.00	9.00	HIGH
Others	8.73	3.12	8.89	8.34	HIGH
Entrepreneurs/Self-employed	4.04	9.00	4.17	4.50	LOW
Legislative & Government Officials	3.93	8.36	4.01	4.29	LOW
NGO/Foundation Managers/Employees (non-legal entities)	3.83	8.14	3.99	4.23	LOW
Religious Leaders	3.75	8.25	3.97	4.22	LOW
Military/Police (including retirees)	3.78	7.50	3.97	4.14	LOW
Political Party Officials	3.81	7.50	3.93	4.13	LOW
Private Sector Employees	3.80	7.39	3.88	4.08	LOW
NGO/Foundation Employees	3.75	7.82	3.81	4.07	LOW
Civil Servants (including retirees)	3.71	7.18	3.86	4.03	LOW
SOE Employees (including retirees)	3.73	7.29	3.83	4.02	LOW
Bank Employees	3.48	6.11	3.65	3.73	LOW
Teachers & Lecturers	3.43	6.11	3.65	3.72	LOW
Students	3.55	5.89	3.50	3.65	LOW
Professionals & Consultants	3.40	5.57	3.50	3.58	LOW
Housewives	3.35	4.82	3.50	3.49	LOW
Money Changers	3.36	4.93	3.47	3.49	LOW
Domestic Workers & Security Guards	3.10	3.64	3.27	3.21	LOW
Farmers & Fishermen	3.05	3.32	3.14	3.11	LOW
Artisans	3.00	3.00	3.00	3.00	LOW

iii. Crowdfunding

In general, the profiles that pose a high ML risk in fintech crowdfunding are legislative and government officials, entrepreneurs/self-employed individuals, civil servants (including retirees), political party officials, and members of the Indonesian National Armed Forces and the National Police (including retirees). Meanwhile, the profiles that pose a high TF risk are entrepreneurs/self-employed individuals, ulama/pastors/leaders of religious organizations and groups, managers/employees of NGOs or other unincorporated organizations, legislative and government officials, political party officials, and members of the Indonesian National Armed Forces and the National Police (including retirees).

Table 40 High-Risk ML Profiles in Fintech Crowdfunding

ML Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Legislative and Government Officials	9.00	9.00	9.00	9.00	HIGH
Entrepreneurs / Self-Employed	8.67	8.73	8.87	8.72	HIGH
Civil Servants (including retirees)	8.28	8.39	8.60	8.33	HIGH
Political Party Officials	7.96	8.12	8.06	7.81	HIGH
TNI/Polri (including retirees)	7.63	7.58	7.85	7.44	HIGH
Private-Sector Employees	6.72	6.84	7.11	6.55	MEDIUM
Employees of SOEs/ROEs (including retirees)	6.59	6.70	6.71	6.25	MEDIUM
Managers/Employees of NGOs or Other Unincorporated Organizations	6.13	6.30	6.71	6.03	MEDIUM
Bank Employees	5.61	5.76	6.03	5.41	MEDIUM
Housewives	5.48	5.49	5.90	5.25	MEDIUM
Managers and Employees of Foundations/Other Unincorporated Legal Entities	5.48	5.76	5.63	5.18	MEDIUM
Professionals and Consultants	5.15	5.22	5.56	4.95	LOW
Money Changer Employees	5.15	5.02	5.36	4.80	LOW
Laborers, Domestic Helpers, and Security Personnel	4.43	4.54	4.89	4.32	LOW
Ulama/Pastors/Leaders of Religious Organizations and Groups	4.17	4.41	4.48	4.06	LOW
Traders	4.30	4.48	4.21	3.98	LOW
Lecturers and Teachers	3.98	4.07	4.55	3.98	LOW
Students	4.11	3.73	3.74	3.59	LOW

Others	3.36	3.00	3.85	3.36	LOW
Farmers and Fishermen	3.00	3.13	3.34	3.12	LOW
Artisans	3.13	3.06	3.00	3.00	LOW

Table 41 High-Risk Profiles for TF in Fintech Crowdfunding

TF Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Entrepreneurs/Self-Employed	9.00	9.00	9.00	9.00	HIGH
Ulama/Priests/Religious Organization Leaders	7.65	8.19	8.33	7.96	HIGH
Managers/Staff of NGOs/Other Unincorporated Organizations	7.84	7.78	7.76	7.56	HIGH
Legislative and Government Officials	7.74	7.37	7.67	7.38	HIGH
Political Party Officials	7.26	7.17	7.67	7.19	HIGH
Military/Police (including retirees)	7.06	6.86	7.76	7.12	HIGH
Private Sector Employees	7.26	7.07	7.29	6.95	MEDIUM
Managers and Staff of Foundations/Legal Entities	6.97	7.27	6.81	6.64	MEDIUM
Civil Servants (including retirees)	6.68	6.56	7.10	6.56	MEDIUM
State-Owned Enterprise Employees (including retirees)	6.48	6.36	6.62	6.20	MEDIUM
Lecturers and Teachers	5.13	5.85	6.14	5.49	MEDIUM
Bank Employees	5.52	5.24	5.76	5.25	MEDIUM
Students	5.90	5.54	5.29	5.16	MEDIUM
Professionals and Consultants	5.32	5.24	5.57	5.11	MEDIUM
Money Changer Employees	4.94	4.63	5.19	4.70	LOW
Housewives	4.94	4.53	5.19	4.68	LOW
Traders	5.32	4.93	4.71	4.61	LOW
Others	3.34	3.14	4.22	3.61	LOW
Laborers, Domestic Helpers, and Security Personnel	3.48	3.41	3.98	3.59	LOW
Farmers and Fishermen	3.48	3.31	3.57	3.39	LOW
Artisans	3.00	3.00	3.00	3.00	LOW

iv. Investment

The profile assessed as high risk for both ML and TF in investment fintech is entrepreneurs/self-employed individuals.

Table 42 High-Risk ML Profile in Investment Fintech

TF Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Entrepreneurs/Self-employed	9.0	9.0	9.0	9.0	HIGH
Private Employees	7.07	7.29	6.55	6.29	MEDIUM
Students	6.85	6.0	6.24	5.85	MEDIUM
Traders	6.72	4.93	6.11	5.58	MEDIUM
Ulama/Priests/Leaders of Religious Organizations and Groups	3.74	8.36	3.89	3.99	LOW
Managers/Employees of NGOs/Unincorporated Organizations	3.77	7.71	3.89	3.94	LOW
Legislative and Government Officials	3.8	7.71	3.85	3.93	LOW
Political Party Officials	3.71	7.07	3.85	3.85	LOW
Armed Forces/Police (including retirees)	3.64	6.86	3.82	3.8	LOW
Managers and Employees of Incorporated Foundations	3.64	7.29	3.72	3.79	LOW
State-Owned Enterprise Employees (including retirees)	3.61	6.64	3.68	3.71	LOW
Civil Servants (including retirees)	3.58	6.43	3.72	3.7	LOW
Lecturers and Teachers	3.39	6.21	3.61	3.59	LOW
Bank Employees	3.42	5.57	3.51	3.5	LOW
Professionals and Consultants	3.39	5.36	3.44	3.44	LOW
Money Changer Employees	3.32	4.71	3.44	3.38	LOW
Housewives	3.32	4.5	3.44	3.36	LOW
Others	3.1	3.23	3.29	3.15	LOW
Laborers, Domestic Helpers, and Security Guards	3.06	3.43	3.24	3.14	LOW
Farmers and Fishermen	3.06	3.21	3.14	3.08	LOW
Artisans	3.0	3.0	3.0	3.0	LOW

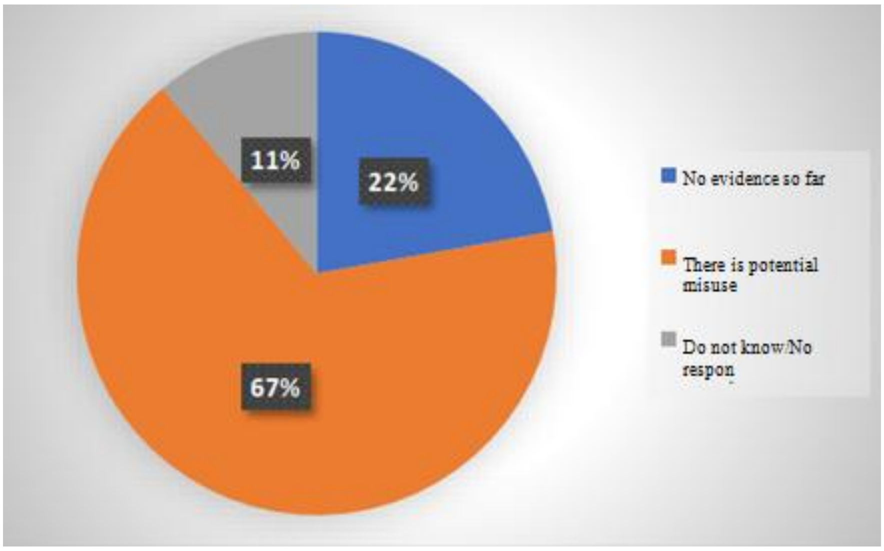
Table 43 High-Risk TF Profiles in Investment Fintech

ML Profile	Threat Scale	Vulnerability Scale	Impact Scale	Risk Scale	Risk Level
Entrepreneurs / Self-employed	9.00	8.51	9.00	9.00	HIGH
Private-sector employees	5.71	6.77	5.45	5.24	MEDIUM
Legislative and Government Officials	4.55	9.00	4.56	4.79	LOW
Civil Servants (including retirees)	4.55	8.30	4.51	4.66	LOW
Homemakers	4.53	5.23	5.12	4.50	LOW
TNI/Police (including retirees)	4.38	7.47	4.29	4.39	LOW
Employees of SOEs/RSOEs (including retirees)	4.56	6.63	4.10	4.22	LOW
Political Party Officials	4.01	7.95	3.81	4.13	LOW
Professionals and Consultants	3.96	5.09	3.74	3.72	LOW
Bank Employees	3.67	5.65	3.70	3.71	LOW
Managers/Employees of NGOs or Other Unincorporated Organizations	3.66	6.07	3.50	3.67	LOW
Managers and Employees of Incorporated Foundations/Organizations	3.46	5.51	3.68	3.65	LOW
Laborers, Domestic Helpers, and Security Personnel	3.70	4.40	3.64	3.54	LOW
Students	4.05	3.84	3.44	3.46	LOW
Traders	3.69	4.12	3.48	3.44	LOW
Teachers and Lecturers	3.64	3.98	3.52	3.43	LOW
Religious Leaders	3.28	4.40	3.40	3.36	LOW
Money Changer Employees	3.44	4.74	3.20	3.35	LOW
Others	3.54	3.02	3.45	3.26	LOW
Farmers and Fishermen	3.37	3.00	3.23	3.15	LOW
Artisans	3.00	3.00	3.00	3.00	LOW

4.3. POTENTIAL RISKS OF FINANCIAL TECHNOLOGY MISUSE IN GENERAL ELECTIONS

Based on INTRAC research conducted in 2019, there is a threat of election campaign fundraising through donation-based crowdfunding mechanisms using virtual accounts. A report published in 2019 by the Association for Elections and Democracy (Perkumpulan untuk Pemilu dan Demokrasi/PERLUDEM), in collaboration with the Westminster Foundation for Democracy (WFD), entitled “The Dynamics of Meeting Campaign Funding Needs of Female Legislative Candidates in the 2019 Simultaneous Elections,” states that public fundraising (crowdfunding) was carried out by several legislative candidates. The report does not record that such crowdfunding activities were conducted through platforms, websites, or applications. According to the report, legislative candidates sent letters or short messages to prospective donors to request financial contributions, and the donors then transferred the funds directly.

Figure 13 Respondents’ Perceptions of the Potential Misuse of Fintech in General Elections



In the context of the 2024 simultaneous general elections, we sought to identify whether there are potential risks of fintech misuse in elections. The majority of respondents (67%) were of the view that there is potential misuse of fintech in elections, although no such cases have been detected to date. Regarding the forms of misuse, respondents believed that potential fintech misuse is most likely to occur during election fund collection and in vote-buying practices (money politics). Examples of potential fintech misuse identified by respondents include:

a. The use of crypto assets to hold election funds or receive donations.
b. The use of digital wallets or electronic money for “dawn attacks” (serangan fajar) and structuring/splitting of transactions.
c. The use of online lending platforms to raise funds.
d. Repayment of online loans on behalf of election candidates by third parties.
e. Collusion between lenders and borrowers in online lending. In online lending or LPBBTI, lenders are required to approve loans to be granted to borrowers. Generally, lenders and borrowers in LPBBTI do not know each other; however, in such cases, lenders and borrowers are acquainted, enabling collusion to occur.

4.4. EMERGING THREATS

We identified several new or emerging threats related to fintech based on respondents' interview responses. These emerging threats include:

a. Payments and Remittances
   i. Transactions using complex layering schemes, for example deposit and withdrawal transactions that do not directly use bank accounts but instead pass through multiple transaction services (including digital wallets and currency conversion websites).
   ii. Misuse of electronic wallets to store and transfer proceeds from online gambling.
   iii. Cash withdrawal and cash deposit features used as a means to break the flow of funds; iv. Cross-border QRIS payments.

b. Lending
   i. Collusion between fund providers and fund recipients in LPBBTI.
   ii. Virtual account payments in LPBBTI transactions that do not use the bank accounts registered under the LPBBTI accounts.

c. Crowdfunding

   For crowdfunding activities, we did not obtain examples of new ML/TF threats from respondents. However, in the context of elections, we identified potential election fund collection through social crowdfunding mechanisms. Crowdfunding is not inherently illegal; however, it may obscure the origin of funds since funding sources come from the public, and it may also potentially exceed individual donation limits.

d. Investment
   i. Crypto asset transactions conducted off-market (transactions on private blockchains or direct person-to-person (P2P) transactions).
   ii. Crypto asset transactions using overseas exchanges.
   iii. Investment through e-commerce platforms, such as online mutual fund investments or gold investments conducted in cooperation with e-commerce platforms.
   iv. Agreements on digital wallet or electronic money transactions conducted through social media (commonly for crypto asset trading).

v. Non-Fungible Tokens (NFTs);

vi. Investment payments made by third parties.

e. Others

i. Creation of fictitious corporate (merchant) accounts used for money laundering activities;

ii. ii. Misuse of buy now, pay later (BNPL) facilities by criminals to purchase goods.

4.5. TYPOLOGIES AND CASE STUDIES

a. Fintech ML and TF Typologies

ML and TF typologies refer to the methods, techniques, schemes, and instruments used by ML and TF perpetrators to conceal, launder, and transfer illicit funds. The Asia/Pacific Group on Money Laundering has identified examples of major ML and TF typologies on its website[14]. The following are several examples of ML and TF typologies that are relevant to fintech:

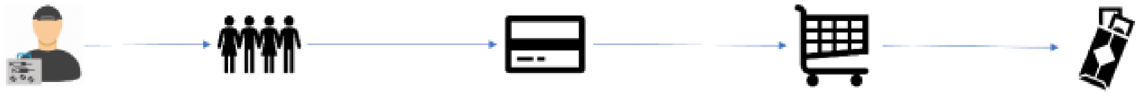
i. Identity fraud/false identity. For example, the use of false identities to obtain loans through fintech lending platforms. Invalid identities may also be obtained through identity theft, both physical and digital, such as through hacking or personal data leaks (data breaches).

ii. Structuring (efforts to avoid reporting requirements by breaking transactions into smaller amounts) and smurfing (efforts to avoid reporting requirements by splitting transactions among multiple actors).

iii. Use of nominees, trusts, family members, or other third parties. In this typology, perpetrators or criminal organizations typically recruit a group of individuals to conduct transactions on their behalf.

[14] **Asia/Pacific Group on Money Laundering (APG).** *Introduction to APG Typologies.* Available at: https://apgml.org/methods-and-trends/page.aspx?p=a4a11dca-75f2-4dae-9c25-6215103e56da

Figure 14. Examples of ML Typologies



Budi and his associates carry out illegal activities(for example, drug trafficking).	Funds obtained from illegal activities are dispersed through multiple channels (for example, cash deposits into bank accounts in small but frequent amounts, purchases of electronic money cards, etc.).	Budi and his associates create multiple accounts using false or stolen information across several platforms to carry out money laundering (for example, peer-to-peer lending platforms or peer-to-merchant).	Using those accounts, Budi and his associates transfer funds through peer-to-peer transactions in small amounts or through the purchase of goods and services, where Budi and his associates act as merchants.	The funds received are then transferred to the bank accounts of Budi and his associates, and subsequently used to acquire assets and luxury goods.

b. Case Studies of ML and TF in Financial Technology

We identified one (1) ML case, two (2) TF cases, and one (1) predicate offense case related to financial technology. The following section discusses these case studies.

a) Money Laundering Case Study

Case 1
Predicate Offense: Fraud Disguised as Foreign Exchange Trading
Based on Court Decision No. 1240/Pid.Sus/2022/PN.Tng

Indra Kesuma, also known as Indra Kenz, registered on the website www.binomo.com (BINOMO) in 2018. The Binomo "game" begins with the player selecting a type of commodity to be predicted, consisting of several options, one of which is foreign currency. After choosing the commodity, the player opens a position by determining the amount of money to be wagered. The player is then required to select a prediction time frame and determine whether the selected commodity will "go up" or "go down." If the player's prediction is correct, they receive a profit of 80% of the wagered amount. If the prediction is incorrect, the player loses 100% of the wagered amount.

Indra Kesuma subsequently became an affiliate of BINOMO. Affiliates recruit prospective players to register on BINOMO and receive profits in the form of affiliate payments based on a percentage of revenue sharing. To increase profits by attracting more members to join BINOMO, Indra Kesuma used several social media channels, including YouTube (IndraKenz), Instagram (@indrakenz), and Telegram (https://t.me/kursustradingidn). In every description of the trading education videos uploaded to his YouTube channel, the Defendant consistently instructed viewers that anyone wishing to trade through the Binomo application/website must use the Defendant's referral link, namely http://www.binomorupiah.com/id, which was included in the video descriptions.

To further convince the public that Binomo was genuinely a legitimate “trading platform,” the Defendant also established PT Kursus Trading Indonesia, a company engaged in education, in which the Defendant acted as Director and majority shareholder. The activities of PT Kursus Trading Indonesia included offering classes or training programs by selling paid educational video services via https://www.kursustrading.com, in which the Defendant provided video-based information related to crypto trading, stocks, financial education, and one of the videos specifically discussed the Binomo game. Course participants were required to pay annual trading course fees ranging from IDR 1,500,000 to IDR 2,000,000 per person, and by early 2022, the courses had attracted approximately 3,000 participants.

Through his social media, the Defendant conveyed a series of false statements, including: “It’s already trusted and Binomo is indeed legal in Indonesia” and “Official in Indonesia since 2015 and already four years running,” whereas in reality, Binomo’s activities were neither legal nor officially licensed in Indonesia, as they had not obtained authorization from the Commodity Futures Trading Regulatory Agency (BAPPEBTI). As a result of the Defendant’s actions, 144 individuals suffered losses totaling approximately IDR 83,365,707,894.

As a Binomo affiliate, the Defendant received profit-sharing payments from Binomo, which were paid through BCA bank accounts in the name of Indra Kesuma, with account numbers 8645057526, 1959990008, and giro account number 1954538888, via several virtual account payment gateways, including PT Fliptech Lentera, PT Intrajasa Teknosolusi, PT Kharisma Catur, PT Dhasatra Money Transfer, Doku, and Dana, as well as through digital crypto assets such as Bitcoin, Ethereum, and others held in the Defendant’s Indodax accounts, either in his own name or in the names of other individuals. The Defendant placed funds received as a Binomo affiliate into his Indodax account under the name INDRA KESUMA in the form of digital currencies, namely Bitcoin and Ethereum. On the INDODAX platform, this amounted to 105 transactions totaling 395.1465503 BTC during the period June 2020 to January 2022. The Defendant subsequently withdrew Bitcoin (BTC), which was liquidated and transferred to bank accounts in the name of INDRA KESUMA via the INDODAX platform, totaling IDR 104,889,343,391. From these affiliate profits, the Defendant purchased various assets, including houses and land, luxury goods such as cars and luxury watches, and transferred funds to the Defendant’s family, romantic partner and her family, other third parties, as well as to PT Kursus Trading Indonesia (the Defendant’s company) and PT BOTX Technology Indonesia.

Indra Kesuma, also known as Indra Kenz, was lawfully and convincingly proven guilty of committing the criminal offenses of spreading false and misleading information resulting in consumer losses in Electronic Transactions and Money Laundering. The Defendant was sentenced to 10 (ten) years of imprisonment and a fine of IDR 5,000,000,000 (five billion rupiah), with the provision that if the fine is not paid, it shall be substituted with 10 (ten) months of imprisonment.

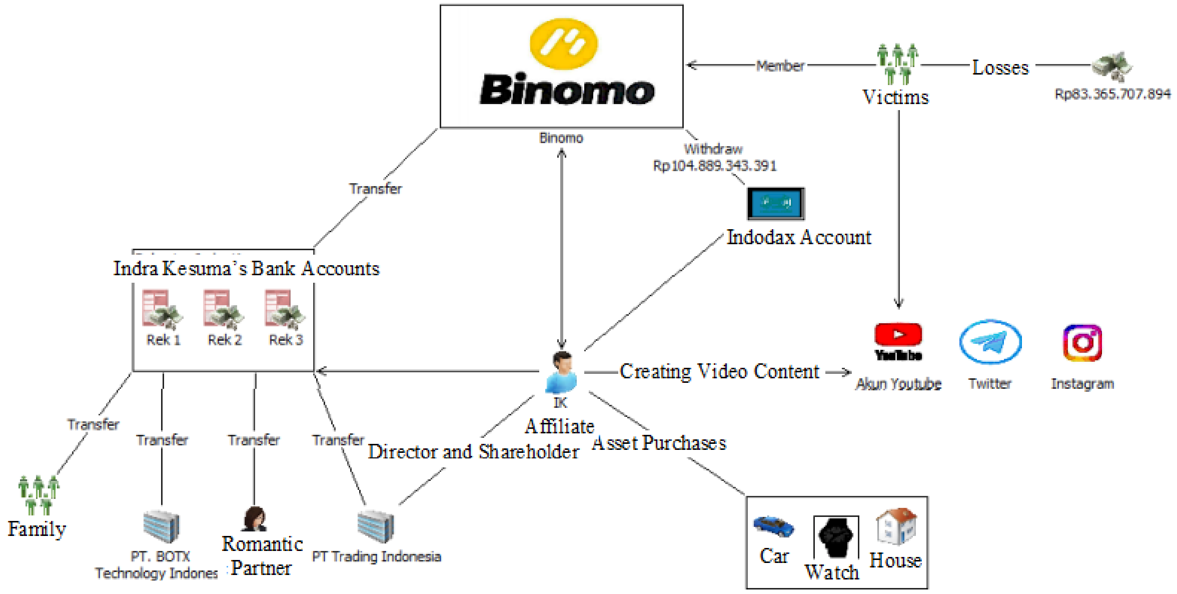


Figure 15 Overview of the Case of Indra Kusuma a.k.a. Indra Kenz

b) Case Study on TF

Case 2
Terrorist Financing through LPBBTI Fintech
Based on Court Decision No. 577/Pid.Sus/2020/PN.JKT.TIM

In 2019, RF planned to carry out an amaliyah operation and required several pieces of equipment. To purchase this equipment, RF and his associates needed funds and therefore obtained loans from Digital Bank Singapore (DS) as well as through several online lending applications. The requirements for borrowing from Digital Bank DS only involved submitting a national identity card (ID Card) and fingerprint scanning. Other online loans with smaller amounts required only an ID Card and a bank account passbook/ATM card. The total amount borrowed by RF was IDR 9,500,000 from Digital Bank DS and approximately IDR 7,750,000 from several financial technology platforms.

The details of loans obtained by RF are as follows:

1. Digital Bank DS: loan application of IDR 10,000,000, disbursed amount IDR 9,500,000.
2. Elastis Pinjam: loan application of IDR 2,000,000, disbursed amount IDR 1,300,000. The loan was not repaid by RF.
3. Rupiah Cepat: loan application of IDR 1,000,000, disbursed amount IDR 500,000.
4. Uang Me: loan application of IDR 1,000,000, disbursed amount IDR 500,000.
5. Tunai Kita: loan application of IDR 1,000,000, disbursed amount IDR 600,000, and fully repaid in the amount of IDR 675,000.
6. Kredit Pintar: loan application of IDR 1,900,000, disbursed amount IDR 2,000,000, and fully repaid in the amount of IDR 2,600,000.
7. Do It: loan application of IDR 1,000,000, disbursed amount IDR 900,000.
8. Cash Cepat: loan application of IDR 1,000,000, disbursed amount IDR 750,000, and fully repaid in the amount of IDR 1,100,000.
9. Pinjam Yuk: loan application of IDR 500,000, disbursed amount IDR 1,000,000, and fully repaid in the amount of IDR 1,750,000.

Subsequently, the loan proceeds were handed over to RF's associate and were used to purchase an air rifle along with its gas cylinder and regulator.

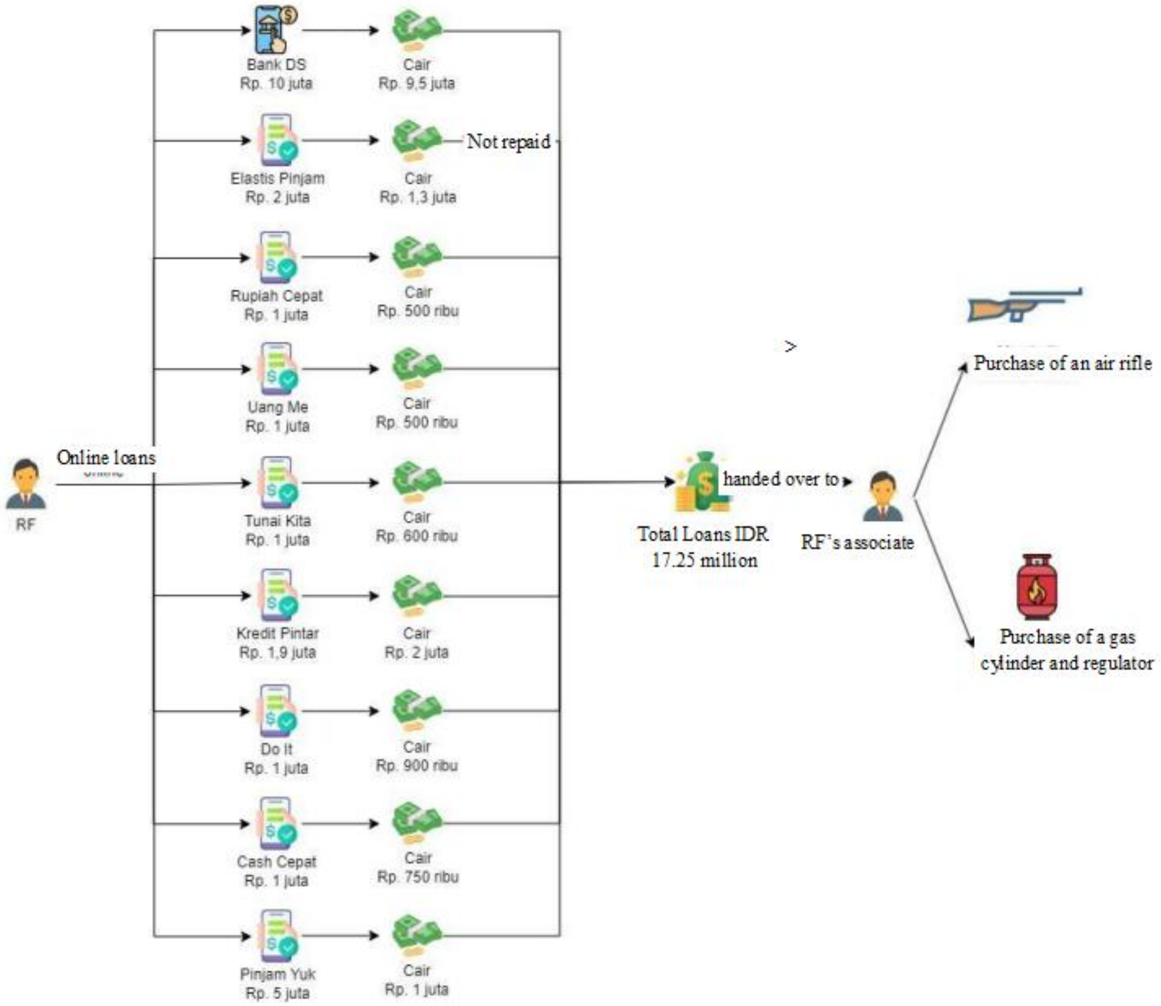


Figure 16 Case Study on the Use of Online Loans

Case 3

TF Financing for Terrorism (TPPT) through LPBBTI Financial Technology Based on Court Decision No. 600/Pid.Sus/2020/PN.JKT.TIM

The defendant committed FAI using a loan-based modus operandi involving Digital Bank DS and online loans from several fintech companies, namely:

a. Bank Digital Singapore (BDS) on 22 April 2019, account number XXX in the name of ADI ALE SAPARI, with a loan amount of IDR 10,000,000, of which IDR 9,420,000 was disbursed.

b. PT Kredit Pintar, under the brand KREDIT PINTAR, on 26 May 2019, with a loan of IDR 600,000, disbursed amounting to IDR 570,000, which was fully repaid by the defendant. Subsequently, on 25 June, the defendant applied for another loan of IDR 600,000, which was disbursed in the amount of IDR 570,000, and has not been repaid to date.

c. PT Kredit Utama Fintech Indonesia, under the brand RUPIAH CEPAT, on 26 May 2019, applied for a loan of IDR 600,000, disbursed IDR 600,000, and fully repaid. On 1 June 2019, applied for a loan of IDR 1,000,000, disbursed IDR 1,010,000, and fully repaid. Subsequently, on 17 June 2019, applied for a loan of IDR 1,330,000, disbursed IDR 1,330,000, which has not been repaid by the defendant to date.

d. PT Digital Kita, under the brand TUNAI KITA, on 22 May 2019, applied for a loan of IDR 2,000,000, which was rejected, and on 30 May 2019, applied for a loan of IDR 1,000,000, which was also rejected.

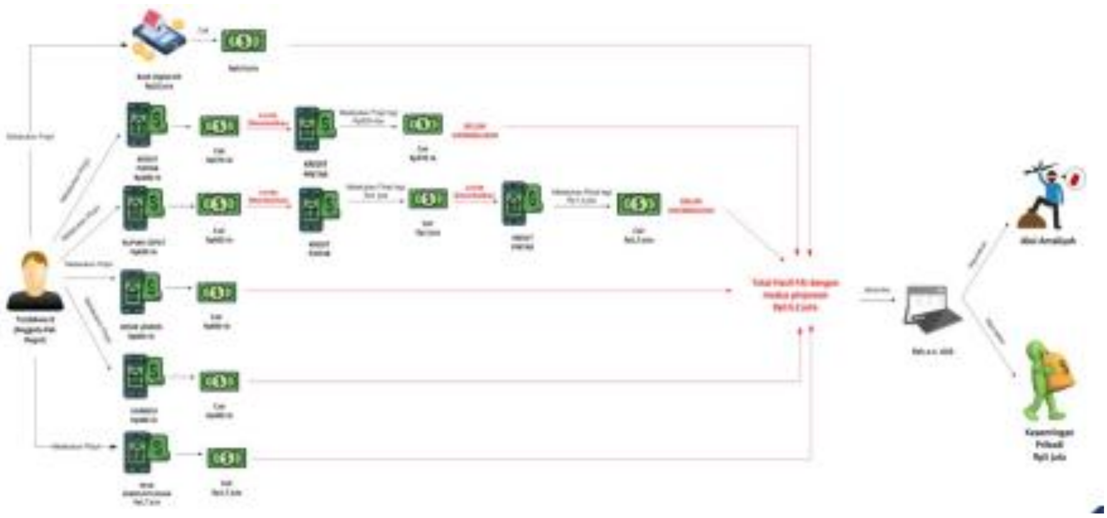
e. PT Kuai Tech Indonesia, using the application PINJAM YUK, on 26 May 2019, applied for a loan of IDR 300,000, but the application was rejected.

f. In addition, the defendant also obtained loans from JERUK LEMON in the amount of IDR 800,000, UANGKU in the amount of IDR 400,000, and PETIK KEBERUNTUNGAN in the amount of IDR 1,700,000.

g. The total amount of money obtained by the defendant from FAI using the loan-based modus operandi amounted to IDR 16,190,000 (sixteen million one hundred ninety thousand rupiah).

The defendant used the said funds for the interests of the "regol" group in order to facilitate the execution of amaliyah actions, and approximately IDR 5,000,000 (five million rupiah) was used for the defendant's personal interests. The disbursement of the loan funds was transferred to a bank account in the name of the defendant, ADI ALE SAPARI.

Figure 17 Case Study on the Use of Online Loans



c) Predicate Offense Case Study

Case 4

Predicate Offense: Fraud Disguised as Crypto Asset Trading
Based on Decision No. 576/Pid.Sus/2022/PN Blb

Doni Salman was found guilty of intentionally disseminating false and misleading information to QUOTEX members, which resulted in consumer losses in Electronic Transactions. The activity or game was presented as if it resembled trading or buying and selling foreign exchange assets or crypto assets/digital currencies such as Bitcoin and Ethereum. The way the platform operated was as follows: members or users who had registered on QUOTEX initially made deposits to a virtual account or via credit card into their QUOTEX member accounts. Subsequently, users could choose products to be played, where QUOTEX provided charts/graphs to be used for analysis (according to the QUOTEX version). Users then selected the amount of funds and determined the time limit for playing on the platform. When users predicted that within a certain period (ranging from 1 minute to 1 day) the price would rise above the current price, they selected the option "UP." If, at the specified time, the price was indeed above the current price, users would obtain a profit of 80% of the amount played. Conversely, if the price was below the current price, users would lose 100% of the amount played.

In March 2021, Doni registered as a trader on the QUOTEX website and also registered as a QUOTEX affiliate, namely a cooperation with QUOTEX to invite and promote QUOTEX to the public so that people would be interested in registering and depositing funds into their QUOTEX accounts. If an affiliate succeeded in inviting between 1 and 14 people to create QUOTEX accounts through the affiliate's registration link, the affiliate would receive profits amounting to 50% of the profits earned by QUOTEX. Profit sharing was conducted using the Revenue Share Model, and affiliates could also choose profits through the Turnover Share Model. Subsequently, Doni created a YouTube account and uploaded video content promoting the registration of QUOTEX accounts affiliated with Doni's affiliate account, promising giveaways in the form of four motorcycles. Doni also showed that he was earning profits when conducting trading or buying and selling shares or currencies on QUOTEX, namely by trading with capital of USD 5,000 (equivalent to IDR 70,000,000). Within two days, Doni claimed to have earned profits amounting to IDR 4,200,000,000 (four billion two hundred million rupiah), which were transferred into his personal bank account. Members of the public who were interested in registering as QUOTEX traders after watching Doni's YouTube account were subsequently added to a Telegram group created and managed by Doni himself under the name GROUP VIP KING SALMANAN. After the members deposited their funds, they followed the playing methods taught by Doni in the group. However, after attempting to play several times, all members continued to fail and incur losses. The price movement charts in the QUOTEX application did not correspond with the price movements shown on tradingview.com (a website that displays charts of various currencies or commodities). Doni continuously encouraged his members to keep topping up their funds by flaunting the assets and wealth he had obtained from his profits, so that Doni could continue to earn profits from members depositing funds into their QUOTEX accounts.

It was subsequently revealed that QUOTEX was a broker platform that did not possess a license and was not registered with the Commodity Futures Trading Regulatory Agency (BAPPEBTI). In addition, QUOTEX was a binary options platform whose transaction activities did not constitute trading, but rather transactions using financial products with mechanisms similar to gambling. Members of the public who registered as QUOTEX traders through Doni's referral link all suffered losses after following the methods provided by Doni, as it was discovered that the transaction mechanism on QUOTEX involved manipulation, whereby at certain moments prior to the final decision, prices were manipulated to cause players' positions to be incorrect and result in member losses. Doni received profits as a QUOTEX affiliate amounting to IDR 40,000,000,000 (forty billion rupiah), or an average of IDR 3,000,000,000 (three billion rupiah) per month from QUOTEX. These funds were obtained by transferring/withdrawing them into Doni's bank account at Bank BCA, account number 8105427111 under the name DONI M. TAUFIK, as well as through an INDODAX account under the name DONI M TAUFIK. Doni subsequently transferred these funds to several other bank accounts. The profits were also used to purchase cars, motorcycles, houses, luxury goods, and to cover daily living expenses. The total losses suffered by victims, based on reports submitted to the Quotex Trading Complaint Post and corroborated by recalculations conducted by accounting experts, amounted to IDR 24,366,695,782, derived from reports submitted by 142 victims.

Doni Muhammad Taufik alias Doni Salmanan was proven legally and convincingly guilty of committing the criminal act of "intentionally and unlawfully disseminating false and misleading information resulting in consumer losses in electronic transactions," as charged in the first primary indictment by the Public Prosecutor. Doni Salmanan was acquitted of the money laundering charge, as stated in the second indictment. Doni Salmanan was sentenced to imprisonment for 4 (four) years and a fine of IDR 1,000,000,000 (one billion rupiah).

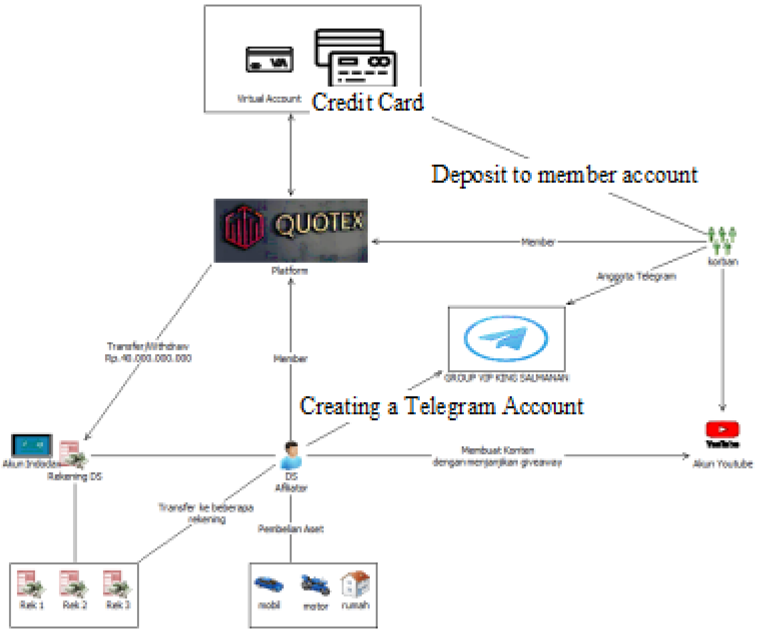


Figure 18 Overview of the Doni Salman Case

CHAPTER V

CONCLUSIONS AND RISK MITIGATION STRATEGIES

5.1. CONCLUSIONS

Based on the results of the identification, analysis, and evaluation of ML and TF risks in the financial technology sector, the following conclusions are obtained:

1. Based on the survey results, the implementation of AML/CFT provisions in fintech is considered stricter than in “conventional” financial institutions and DNFBPs because fintech has already adopted the latest technologies, for example integration with population data and biometric data such as face recognition technology. In addition, for Crypto Asset service providers, there are several software tools capable of conducting transaction monitoring, such as Chain Analyst. From the supervision and regulatory perspective, there is on-site and off-site supervision and an obligation to submit periodic reports to regulators.
2. Based on the survey results, respondents tend to believe that the impact arising if ML and TF occur in fintech will be greater compared to “conventional” financial institutions and DNFBPs.
3. Based on the results of the identification, analysis, and evaluation of Money Laundering (ML) risks in financial technology (fintech), the following conclusions are obtained:
    a. In the ML risk mapping, the fintech types with high risk are investment and remittance and payment.
    b. In general, predicate offenses identified as posing high ML risk based on fintech types (lending, investment, remittance and payment, and crowdfunding) are fraud.
    c. In the mapping of ML typology risks in financial technology, the high-risk typologies are asset purchases, structuring (breaking transactions into smaller nominal amounts but conducted multiple times by one person), and smurfing (breaking transactions conducted by several people).
    d. Based on fintech types, the following ML typology risk mapping is identified:
        a) Based on payment and remittance fintech types, the high-risk ML typologies are structuring (breaking transactions into smaller nominal amounts but conducted multiple times by one person), smurfing (breaking transactions conducted by several people), and asset purchases.
        b) Based on lending fintech types, the high-risk ML typologies are structuring (breaking transactions into smaller nominal amounts but conducted multiple times by one person), smurfing (breaking transactions conducted by several people), asset purchases (property,

vehicles, etc.), and luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.).

c) Based on investment fintech types, the high-risk ML typologies are structuring (breaking transactions into smaller nominal amounts but conducted multiple times by one person), smurfing (breaking transactions conducted by several people), asset purchases (property, vehicles, etc.), luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.), and mingling (mixing legal and illegal funds).

d) Based on crowdfunding fintech types, the high-risk ML typologies are structuring (breaking transactions into smaller nominal amounts but conducted multiple times by one person), smurfing (breaking transactions conducted by several people), asset purchases (property, vehicles, etc.), and luxury goods purchases (jewelry, gold, luxury bags, luxury cars, etc.).

e. In the mapping of Predicate Offenses (PC) specifically based on fintech types, the following are identified:

a) Based on payment and remittance fintech types, predicate offenses posing high ML risk are gambling and corruption.

b) Based on lending fintech types, predicate offenses posing high ML risk are narcotics, fraud, and gambling.

c) Based on crowdfunding fintech types, predicate offenses posing high ML risk are fraud.

d) Based on investment fintech types, predicate offenses posing high ML risk are fraud.

f. In general, regions posing high ML risk in financial technology are DKI Jakarta. This is because most fintech companies have their headquarters in DKI Jakarta, and a very large number of fintech transactions occur in DKI Jakarta as the center of government and business.

g. ML risk mapping in financial technology based on regions is as follows:

a) Based on payment and remittance fintech types, regions posing high ML risk are DKI Jakarta.

b) Based on lending fintech types, regions posing high ML risk are DKI Jakarta, East Java, and West Java.

c) Based on crowdfunding fintech types, regions posing high ML risk are DKI Jakarta and East Java. Based on investment fintech types, regions posing high ML risk are DKI Jakarta.

h. In general, profiles posing high ML risk in financial technology are entrepreneurs/self-employed individuals.

i. Based on fintech types, profiles posing high ML risk are as follows:

a) Entrepreneurs/self-employed individuals, private-sector employees, housewives, and civil servants (including retirees) are profiles posing high ML risk in payment and remittance fintech types.

b) Private-sector employees and entrepreneurs/self-employed individuals are profiles posing high ML risk in lending fintech types.

c) Legislative and government officials, entrepreneurs/self-employed individuals, civil servants (including retirees), political party officials, and TNI/Polri (including retirees) are profiles posing high ML risk in crowdfunding fintech types.

d) Entrepreneurs/self-employed individuals are profiles posing high ML risk in investment fintech types.

4. Meanwhile, based on the results of the identification, analysis, and evaluation of Terrorist Financing (TF) risks in financial technology, the following conclusions are obtained:
    a. In the risk mapping, the fintech type posing high TF risk is lending.
    b. According to respondents' perceptions, profiles posing high TF risk in fintech based on TF stages are the use of funds for domestic terrorist operations using false identity documents and the legal fundraising stage through personal sponsors (terrorist financiers/fundraisers), diversion of donation collection through mass organizations, crowdfunding financing, legitimate business activities, and self-funding.
    c. Payment and remittance, crowdfunding, investment, and lending fintech types pose high risk of being used for TF stages, namely the use of funds for domestic terrorist operations using false identity documents and the legal fundraising stage through personal sponsors (terrorist financiers/fundraisers), diversion of donation collection through mass organizations, crowdfunding financing, legitimate business activities, and self-funding.
    d. In general, regions posing high TF risk in financial technology are DKI Jakarta and West Java.
        e. TF risk mapping in financial technology based on regions is as follows:
        a) Based on payment and remittance fintech types, regions posing high TF risk are West Java.
        b) Based on lending fintech types, regions posing high TF risk are West Java.
        c) Based on crowdfunding fintech types, regions posing high TF risk are DKI Jakarta, West Java, and East Java.
        d) Based on investment fintech types, regions posing high TF risk are West Java.
    f. In general, profiles posing high TF risk in financial technology are traders and entrepreneurs/self-employed individuals.
    g. Based on fintech types, profiles posing high TF risk are as follows:
        a) Private-sector employees and students are profiles posing high TF risk in payment and remittance fintech types.
        b) Traders and others are profiles posing high TF risk in lending fintech types.
        c) Entrepreneurs/self-employed individuals, ulama/pastors/leaders of religious organizations and groups, managers/employees of NGOs/unincorporated organizations, legislative and government officials, political party officials, and TNI/Polri (including retirees) are profiles posing high TF risk in crowdfunding fintech types.
        d) Entrepreneurs/self-employed individuals are profiles posing high TF risk in investment fintech types.

5.2. RISK MITIGATION STRATEGIES

Based on the results of the identification of threats, vulnerabilities, and impacts, as well as the risks of Money Laundering crimes and Terrorist Financing crimes in Fintech, a risk evaluation has been conducted and risk mitigation strategy measures have been determined that can be implemented by all relevant stakeholders, including:

a. **Prevention Sector**

No.	Prevention Strategy	Term	Responsible Parties
1	Capacity building of human resources	Medium	1. Reporting Parties 2. SR Authorities 3. LEA 4. INTRAC
2	Strengthening compliance with the implementation of AML/CFT regulations by Fintech operators	Short	1. Reporting parties 2. SR Authorities
3	Strengthening supervision of Fintech by SR Authorities	Short	1. SR Authorities 2. Reporting parties
4	Improving stakeholder socialization on ML and TF threat awareness in Fintech	Medium	1. SR Authorities 2. Reporting parties
5	Optimization of guidelines and training on identification of suspicious transactions (TKM) and STR quality (LTKM)	Medium	1. SR Authorities 2. Reporting parties
6	Strengthening reporting roles on perpetrator data by Fintech business actors	Medium	1. SR Authorities 2. Reporting parties
7	Increasing personnel handling ML and TF related to Fintech	Long	LEA

b. Eradication Sector

N.	Eradication Strategy	Term	Responsible Parties
1	Enhancing information exchange between Fintech Supervisory Authorities and Law Enforcement Apparatus	Short	1. SR Authorities 2. LEA 3. INTRAC
2	Improving Law Enforcement Apparatus' understanding of Fintech	Medium	1. SR Authorities 2. LEA
3	Accelerating the provision of infrastructure and facilities for crypto asset analysis	Long	1. LEA 2. INTRAC
4	Strengthening the enforcement of sanctions against illegal Fintech activities	Short	1. SR Authorities 2. LEA

c. Cooperation Sector

N.	Cooperation Strategy	Term	Responsible Parties
1	Enhancing data and information exchange related to supervision and typologies	Short	1. SR Authorities 2. LEA 3. INTRAC
2	Strengthening cooperation between authorities and Fintech industry associations to enhance AML/CFT program implementation	Medium	1. SR Authorities 2. Fintech Industry Associations
3	Strengthening cooperation between authorities and the Financial Intelligence Unit to conduct fit and proper assessments of Fintech management	Medium	1. SR Authorities 2. INTRAC
4	Strengthening cooperation between authorities and law enforcement apparatus in investigations involving Fintech providers	Medium	1. LEA 2. SR Authorities 3.
5	Strengthening cooperation with international counterparts (FIUs, LEAs) or international Fintech associations	Long	1. SR Authorities 2. LEA 3. INTRAC

6	Strengthening cooperation between Fintech service providers, financial institutions, and supervisors to develop higher AML/CFT standards within a Public–Private Partnership framework	Long	1. SR Authorities 2. Reporting Parties (Fintech and Non-Fintech) 3. LEA 4. INTRAC

REFERENCES

Annur, Cindy Mutia. (2022). “Securities Crowdfunding Funds Reached IDR 507 Billion as of June 2022.” Accessed from https://databoks.katadata.co.id/datapublish/2022/06/09/dana-securities-crowdfunding-tembus-rp507-miliar-per-juni-2022

Asosiasi Fintech Pendanaan Bersama Indonesia. “History of Fintech Development in Indonesia.” Accessed from https://afpi.or.id/articles/detail/sejarah-perkembangan-fintech-di-indonesia

Asia Pacific Group on Money Laundering. *Introduction to APG Typologies.* Accessed from https://apgml.org/methods-and-trends/page.aspx?p=a4a11dca-75f2-4dae-9c25-6215103e56da

Asia Pacific Group on Money Laundering. (2023). *2023 APG Typologies Report.* Accessed from https://apgml.org/includes/handlers/get-document.ashx?d=72202b2a-c616-472e-be60-c53fdd810def

Bank Indonesia. (1 December 2018). “Understanding Financial Technology.” Accessed from https://www.bi.go.id/id/edukasi/Pages/mengenal-Financial-Teknologi.aspx

Bank Indonesia. (31 March 2023). “Digital Wallets Gain Popularity, Attracting Interest During the Pandemic.” Accessed from https://www.bi.go.id/id/bi-institute/BI-Epsilon/Pages/Dompet-Digital-Naik-Daun,-Membetot-Minat-Kala-Pandemi.aspx

Bank Indonesia. “Indonesian Financial System Statistics.” Accessed from https://www.bi.go.id/id/statistik/ekonomi-keuangan/sski/default.aspx#headingOne

Europol. (2023). *European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime.* Publications Office of the European Union, Luxembourg. Accessed from https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf

Financial Action Task Force. (2023). *Crowdfunding for terrorist financing.* Accessed from https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html

Mumpuni, Melvin. (2022). *Comparison of How Conventional P2P Lending Works vs. Sharia P2P Lending.* Accessed from https://www.finansialku.com/ini-lho-cara-kerja-p2p-lending-konvensional-dan-p2p-lending-syariah/

Otoritas Jasa Keuangan. “Fintech Lending FAQ.” https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/direktori/fintech/Documents/FAQ%20Fintech%20Lending.pdf

Tanamduit Team. (2023). “Top 10 Best and Most Trusted Mutual Fund Investment Applications.” Accessed from https://www.tanamduit.com/belajar/reksa-dana/aplikasi-investasi-reksadana

APPENDICES

International Case Studies

a. Remittances and Payments

Case 1
Remittances for the Transfer of "Ransom" Funds

In an online fraud case in 2022, fake correspondence was sent via email and social media, purportedly from Europol departments and senior staff. The messages informed victims that they had visited websites hosting child sexual abuse material and urged them to reply to the email address provided. Respondents were instructed to make payments ranging from EUR 3,000 to EUR 7,000 via bank transfers or instant money services to avoid prosecution.
Source: Europol

Case 2
Laundering of Proceeds from Sexual Exploitation through the Use of Stored Value Facilities (SVF)[15] – Hong Kong

In 2022, an investigation into a local proxy syndicate that arranged women to provide illegal sexual services found that the syndicate received service fees from customers in cash. Approximately USD 35,000 in cash was subsequently deposited into stored value facility accounts held by the syndicate's money mules, before being transferred to the syndicate. Two syndicate members were arrested at the end of 2022 for legal violations by law enforcement authorities. Investigations into this case are still ongoing.
Source: APG

b. Crowdfunding

Case 3
Terrorist Financing through Social Crowdfunding – Germany

In 2020, Germany issued a sectoral risk assessment on terrorist financing through the misuse of non-profit organisations (NPOs), which found that developments in Germany's non-profit sector allowed more flexible fundraising methods, for example through online platforms and crowdfunding initiatives. This may lead to anonymity, making it more difficult for authorities and potential donors to review the activities of related organisations. Germany acknowledged that such an environment could become attractive to terrorist organisations, which may seek to exploit it. ISIS and Salafi organisations in Germany were known to be involved in crowdfunding activities, and there were several cases in which registered charities were used to raise funds for terrorist financing under the guise of collecting donations for crisis areas in Syria/Iraq.
Source: FATF

[15] *Stored Value Facilities (SVF)* is a term used in Hong Kong for payment system service providers, which include electronic wallets and electronic money cards.

Case 4
Use of Social Crowdfunding by ISIS Financiers – Canada

In July 2023, following an investigation led by the Royal Canadian Mounted Police (RCMP), Khalilullah Yousuf was charged with terrorism-related offences for allegedly being part of an international network supporting ISIS that used online and encrypted messaging platforms to provide recruitment and financial support to ISIS. The investigation revealed that Yousuf created and disseminated pro-ISIS propaganda on social media with the aim of radicalizing and recruiting individuals into the terrorist group. Yousuf is also alleged to have conspired with ISIS members abroad to carry out terrorist attacks against foreign embassies in Afghanistan, as well as to have provided propaganda and research related to attacks carried out in Afghanistan against foreign nationals. Working together with other co-conspirators, Yousuf created various fundraising campaigns on crowdfunding platforms, falsely claiming to raise funds for charitable purposes. Other financial intermediaries and virtual accounts (VA) were also used to collect and transfer the proceeds. Yousuf was charged with:

- providing property and services for terrorist purposes, contrary to Section 83.03 of the Canadian Criminal Code;
- participation in the activities of a terrorist group, contrary to Section 83.18 of the Canadian Criminal Code; and
- facilitating terrorist activity, contrary to Section 83.19 of the Canadian Criminal Code.

International cooperation was critical for the RCMP to uncover the full scope of the illicit activities and to identify key individuals involved in the scheme. The criminal investigation is ongoing and has been brought before the courts. Criminal charges against Yousuf and three other individuals have also been filed in the United States.

Source: FATF

c. Investment

Case 5
Money Laundering through Crypto Asset Service Providers

In January 2023, law enforcement authorities shut down a crypto platform suspected of being used by criminals to launder illicit funds belonging to Russian entities under EU sanctions. Bitzlato allowed the rapid conversion of various crypto assets such as bitcoin, ethereum, litecoin, bitcoin cash, dash, dogecoin, and tether into Russian rubles. It is estimated that the crypto exchange platform received assets with a total value of EUR 2.1 billion (BTC 119,000). Although the conversion of crypto assets into fiat currency is not illegal, investigations into cybercriminal operators revealed that a large volume of criminal assets passed through the platform. Analysis showed that approximately 46% of the assets exchanged through Bitzlato, valued at around EUR 1 billion, were linked to criminal activity.

Source: Europol

Case 6
Crypto Asset Investment Fraud Using a Ponzi Scheme

A criminal network used the social media platform Vitae.co and the website Vitaetoken.io to deceive individuals into investing in a cryptocurrency Ponzi scheme. Approximately 223,000 people from 177 countries are believed to have been victimized. Members of the criminal network included Belgian nationals who used companies under Swiss jurisdiction. More than EUR 1 million in cash was seized, along with crypto assets worth EUR 1.5 million and 17 luxury vehicles.

Source: Europol

Case 7
International Money Laundering Syndicate – Australia

In 2023, nine individuals were arrested in connection with an alleged Money Laundering Organization (MLO) valued at AUD 10 billion. The investigation originated from an earlier arrest of suspects carrying large amounts of cash and extensive tracing of proceeds of crime. The nine individuals allegedly traded in criminal proceeds, used foreign and domestic shell companies to launder funds, and submitted fraudulent bank loan applications. The MLO was linked to suspicious international transfers and allegedly used professional facilitators, including accountants and bank staff, to apply for loans from domestic banks and use the funds to finance real property acquisitions and mortgage payments.

Significant domestic cooperation involved the Criminal Assets Confiscation Taskforce (CACT), the Australian Federal Police (AFP) money laundering taskforce AVARUS, AUSTRAC, the Australian Taxation Office (ATO), the Australian Securities and Investments Commission (ASIC), and the Department of Home Affairs. International cooperation with foreign law enforcement apparatus was also conducted through the AFP’s international policing networks.

The AFP restrained assets valued at AUD 200 million. The restrained assets included crypto assets worth AUD 30 million, 18 designer watches, 17 designer handbags, at least 46 luxury jewellery items, 20 real properties, 66 bank accounts, and five luxury vehicles.

The nine individuals were charged with money laundering offences under the Criminal Code 1995 and the Anti-Money Laundering and Counter-Terrorist Financing Act 2006. Confiscation proceedings under the Proceeds of Crime Act 2002 (Cth) are ongoing.

Source: APG

Case 8
Crypto Asset Embezzlement – Hong Kong

Person A was a financial operator at a FinTech company, with duties including managing the company's crypto accounts. Person A abused this position by transferring USD 3.2 million (equivalent to HKD 25.6 million (USD 3.3 million)) to personal crypto wallets belonging to himself and his relatives. The stolen crypto assets were then exchanged into other crypto assets and transferred back and forth between Person A and his associate.

Eventually, crypto assets worth approximately HKD 18 million were converted into fiat currency and deposited into Person A's personal bank account, while other crypto assets were transferred to other crypto wallets. Person A and his associate subsequently purchased two residential properties and a new vehicle. In mid-2022, the FinTech company conducted an internal audit and uncovered the embezzlement committed by Person A. Person A and two associates were arrested by the Hong Kong Police and charged with theft. Person A's bank account containing HKD 2 million and crypto assets worth HKD 6 million were seized. The investigation is ongoing.

Source: APG

Case 9
Disguising Money Laundering Activities as Crypto Transactions – Hong Kong

An investigation by the Hong Kong Police revealed that a fraud syndicate exploited 136 bank accounts belonging to the syndicate or money mules to launder proceeds amounting to HKD 27 million derived from various types of fraud. The tainted funds were commingled within these accounts or used in crypto asset trading before ultimately being withdrawn in cash from ATMs. In mid-2022, 16 individuals, including core syndicate members, were arrested for money laundering, and HKD 5.5 million was seized. The investigation is ongoing.

Source: APG

Case 10

Crypto Asset Fraud through a Dating Website – Japan

Person A and a group of associates developed worthless crypto assets as fundraising tokens to invest in fictitious overseas businesses. A victim was deceived into investing in crypto assets by a group posing as a female investor on a dating website. The victim used 42 Bitcoin and 1.4 million Ripple to purchase the fake crypto assets.

The group subsequently transferred the fraudulently obtained crypto assets through two additional coin wallets and a crypto broker before converting the crypto assets into cash.

Source: APG

Case 11

Proceeds of Computer Fraud Concealed through Crypto Asset Transfers – Japan

Person B committed computer fraud and transferred bitcoin to Person C, an individual under his control. Person C transferred the bitcoin to Person A in exchange for a cash payment of JPY 209 million (approximately USD 1.4 million). Person A concealed 41.28 bitcoin in March 2021 by storing them in a wallet registered under the name of Person D but controlled by Person A.
Person A was arrested and prosecuted for violating the Act on Punishment of Organized Crimes (Concealment of Criminal Proceeds).

Source: APG

Case 12

"Omnis Gold" Internet Fraud – South Korea

This case involved fraud in which perpetrators deceived 141 victims, causing losses of approximately KRW 35.9 billion (around USD 26.46 million). The fraud involved deceiving victims into accumulating points through a smartphone application and purchasing "Omnis Gold" coins with the promise of receiving a 4% return on their investment. The FIU facilitated the investigation by providing financial transaction reports to the investigative police office. Through swift and mandatory investigations, prosecutors and police substantiated the offences committed by the perpetrators and successfully arrested all of them. Prosecutors and relevant authorities identified the financial gains obtained by the perpetrators, and the Court approved seizure orders prior to prosecution against general property (not directly linked to the crime) owned by the perpetrators, thereby contributing to the recovery of funds on behalf of the victims.

Source: APG

Case 13

Using Proceeds of Telecommunications Network Fraud to Purchase Crypto Assets – Macau

In late March 2022, the Judiciary Police of Macau, China, received notification from counterparts in a foreign jurisdiction that a criminal syndicate was involved in cross-border crypto asset money laundering activities. After in-depth investigation, it was found that the syndicate used part of the proceeds of internet telecommunications fraud to purchase crypto assets and launder the money through local telecommunications shops.

Based on the investigation, the criminal syndicate began operating in October 2020. The syndicate instructed its subordinates to open approximately 180 bank accounts in Jurisdiction A, specifically to receive and handle illegal proceeds originating from telecommunications fraud committed locally and in several other countries, as well as to receive large sums of funds of unknown origin. Since July 2021, the criminal syndicate ordered several of its members to travel to Macau, China, to withdraw cash from

ATMs using bank cards issued by Jurisdiction A. Subsequently, crypto assets were purchased through telecommunications shops and resold on overseas VASP trading platforms. The proceeds from the sale of crypto assets were then withdrawn in cash in Macau, China, thereby achieving the objective of money laundering. Bank accounts in different jurisdictions owned by the criminal syndicate were used to handle suspicious funds totaling approximately USD 141 million, while syndicate members in Jurisdiction A and Macau, China, withdrew a total of USD 46 million.

A joint operation between the Judiciary Police and law enforcement authorities of Jurisdiction A was conducted. Judiciary Police officers intercepted two suspects from Jurisdiction A at a hotel, while two suspects from Macau, China, and another suspect from Jurisdiction B were intercepted at an apartment and a telecommunications shop.

The Judiciary Police investigation revealed that the two suspects from Jurisdiction A had withdrawn cash approximately 1,000 times from ATMs in Macau, China, since December 2021, with a total amount of cash withdrawn reaching USD 3.6 million. Their bank accounts received a total of USD 242,000 derived from 12 fraud cases.

The duo simultaneously admitted that they used their own bank cards as well as the bank cards of relatives and friends to withdraw cash and assisted criminals from Jurisdiction A in conducting crypto asset transactions through overseas crypto asset platforms. One suspect from Macau, China, and another suspect from Jurisdiction B were staff members of a telecommunications shop.

The Judiciary Police arrested and transferred the above suspects to the Public Prosecutor’s Office on charges of criminal association and money laundering, while continuing to pursue other individuals involved.

Source: APG

Case 14

Transferring Crypto Assets from Another Person’s Wallet Using Malicious Software – Mongolia

In July 2021, Person B hacked the victim’s personal computer using malicious software and stole 32.7 Ethereum from the victim’s crypto asset wallet. The 32.7 Ethereum was then transferred to a domestic VASP through 26 blockchain transactions divided into six portions. Subsequently, 23.45 Ethereum was transferred to a blockchain wallet and then transferred to Person D’s account at a foreign VASP.

Person D is the younger sister of Person B, the aforementioned cyber attacker, and Person B converted the hacked Ethereum into Bitcoin and other crypto assets to conceal its origin using his sister’s account. He then transferred the crypto assets to Persons M, N, and O, who are friends of Person B. After that, MNT 65 million was transferred to Person E, who committed the crime jointly.

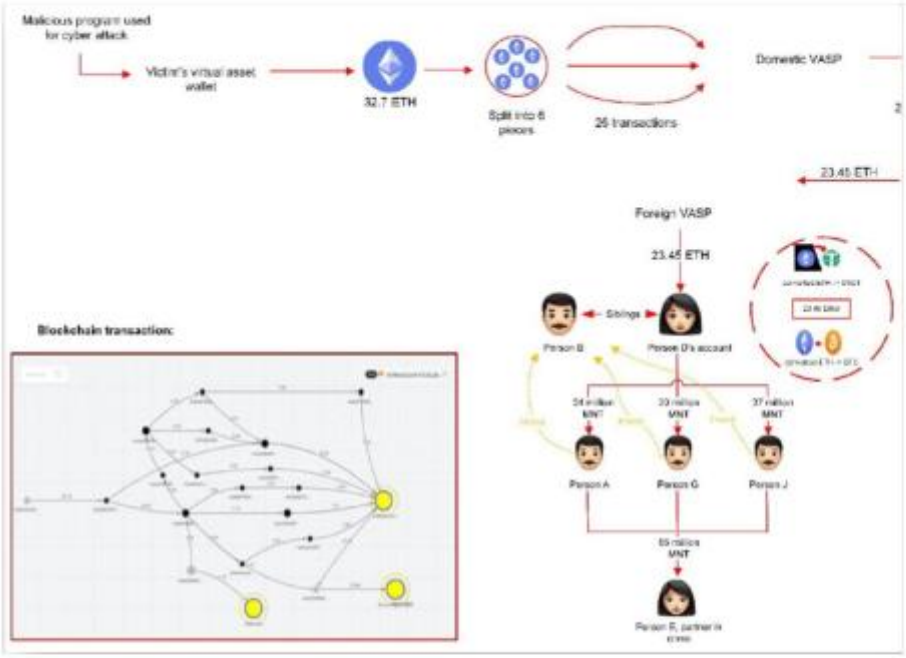
During the investigation, investigators discovered 0.5 Bitcoin in Person D’s account at the foreign VASP, which was the remaining amount of crypto assets from the conversion of the stolen Ethereum, and subsequently froze Person D’s account at the foreign VASP.

Person B paid full restitution at the trial stage; in October 2022, he was sentenced to 2 years and 6 months of imprisonment under the articles “Illegal Invasion of Electronic Information,” “Developing and Selling Programs and Devices for Illegal Invasion of Electronic Information Networks,” and “Money Laundering” in the Mongolian Criminal Code.

In January 2023, the Criminal Court of Appeal upheld Person B’s sentence.

Source: APG

Figure 19 Overview of Case 14



Case 15

Bitcoin Trader Facilitating Fraud – New Zealand

A peer-to-peer bitcoin trader operating on localbitcoins.com facilitated the conversion of fraudulently obtained fiat currency into bitcoin on behalf of international fraudsters operating overseas. The overseas fraudsters contacted victims residing in New Zealand and engaged in fraudulent practices (primarily romance scams and “advance-fee” scams) to persuade victims to give them money. The fraudsters instructed their victims to meet their local “associate” (the bitcoin trader) to hand over cash, thereby providing the victims with a time and place to meet the associate.

Meanwhile, the fraudsters also contacted the bitcoin trader and informed them that they wished to purchase bitcoin using NZD, instructing the trader to meet their “associate” (who was in fact the fraud victim) at a specified time and place to carry out the exchange. The fraudsters provided the trader with their bitcoin wallet address, to which the trader would credit bitcoin equivalent to the amount of cash handed over by the victim. The bitcoin trader conducted no form of CDD when facilitating these trades, accepted cash from the victims, and credited bitcoin to the fraudsters on a “no questions asked” basis.

Source: APG

Case 16

Ponzi Scheme Using an Online Platform – Pakistan

This complex online fraud offence was identified by law enforcement in January 2021.

The FMU also received STRs and disseminated its analysis relating to the group referred to below (Group A&B) in early 2021, highlighting concerns regarding the operations of the companies and their accounts.

Persons A and B were the principal suspects involved in a Ponzi scheme responsible for defrauding members of the public of PKR 17 billion (USD 94.4 million) between January 2019 and February 2021. They developed Group A&B and, with the assistance of other individuals, maintained the Group A&B web portal, which purported to offer investment opportunities with returns ranging from 7% to 20% per month.

The companies solicited investments by claiming to be engaged in property transactions; crypto exchanges; information technology; transportation services and trading; however, they never carried out such investments. Funds from new customers were used to finance interest payments to existing "investors," thereby creating a Ponzi scheme. It is estimated that 50% of new deposits were diverted to pay interest to existing investors and agents employed to recruit new investors. Payments from the online platform were routed through the Group A&B companies.

Group A&B consisted of 26 companies established by Person A and registered in the names of family members, including his son, cousin, and two wives within the family group.

Investigations with the SECP revealed that these companies did not hold official authorisation to solicit deposits from the public, and therefore their activities were illegal.

The investigation linked 70 bank accounts of the accused, their relatives, unregistered companies, and SECP-registered companies, maintained across several commercial banks throughout Pakistan since 2019. Analysis of these accounts was conducted with the assistance of banking experts, establishing how the scheme laundered proceeds of crime through these accounts into the personal and investment accounts of Person A and his associates. Details of these accounts were obtained from the Central Bank, and more than 50,000 transactions were analysed.

Asset tracing investigations established that the proceeds of crime had been used to purchase 31 immovable properties and 30 movable properties with an estimated value of PKR 6.7 billion (USD 37.2 million).

In September 2021, APH formed an investigation team led by the AML/CFT Directorate, Islamabad, with a senior investigator and lead investigator appointed. Computer forensic experts facilitated the recovery and analysis of complex databases that enabled investments to be transacted through a layered false referral scheme. The databases were stored in the cloud and required expert assistance to retrieve. The databases contained more than 1,000,000 transactions reconciled with payments to the A&B accounts.

Family trees and related data were collected from the National Database and Registration Authority, and travel histories of the accused were obtained to support the investigation. Information and evidence shared by the FMU and SECP, as well as records from various commercial banks via the State Bank of Pakistan (SBP), also assisted the investigation.

Interpretation of data retrieved from the suspects' websites indicated that the suspects had conducted similar fraudulent business activities in Jurisdictions B and C. Financial investigations also suggested that proceeds of crime were transferred to Jurisdiction D, where a request for international cooperation has been sent. International cooperation is also ongoing to trace assets in Jurisdictions B and C and to track the suspects' associates there.

Investigative techniques employed during the AML investigation included forensic accounting, digital forensics, social engineering of social media profiles, analysis of banking records, interviews, and seeking assistance from international jurisdictions.

The SECP has also concluded judicial proceedings against the Group and its sponsors for illegally collecting deposits from the public and operating pyramid schemes, in violation of the Companies Act, 2017. The Group comprised 18 companies incorporated under the Companies Act, 2017, as well as five unrelated business establishments. The principal sponsor of the Group was Person A, along with his close family members. Upon completion of legal proceedings, the SECP disqualified the Group's sponsors from serving as directors of any company for a period of five years and imposed a fine of PKR 100 million on each sponsor. Furthermore, the sponsors were prohibited from establishing new companies under the Companies Act, 2017.

Source: APG

Case 17

Bitcoin Trader Facilitating Fraud – Pakistan

An STR was reported by Bank A on the account of Person A due to suspected involvement in illicit crypto-asset transactions. Activity on the crypto-asset trading platform revealed that Person A was involved in the sale and purchase of Bitcoin, which is illegal in Pakistan in accordance with Central Bank instructions. Bank A investigated Person A's account due to reported unusual transactional activity arising from high account turnover and transactions with unrelated counterparties. During the analysis of transactional activity, it became clear that the individual was involved in crypto-asset trading.

Subsequently, Person A conducted high-value transactions with various unrelated parties, most of whom were suspected of being involved in Hawala or other criminal activities. The FIU Pakistan database identified one of Person A's counterparties, Person B, the owner of Business X, who was found during an investigation by the Anti-Narcotics Force to have obtained proceeds from the sale of narcotics. Person B's account was credited with large sums of money from Person A's account without a clear purpose.

Financial intelligence was shared with law enforcement apparatus and the central bank, as Person A was suspected of engaging in crypto-asset transactions and possibly facilitating others in channeling proceeds of crime using crypto assets.

Source: APG

Case 18

Crypto-Asset Theft – Philippines

Person A was the project director of a non-profit organization suspected by law enforcement of being involved in TF by supporting the activities of a group in the southernmost part of the Philippines. Person A's crypto account at VASP C received crypto assets (mostly bitcoin) from more than 300 external crypto wallets and other crypto accounts at VASP C, amounting to approximately PHP 856,000 (around USD 15,309). The funds were accumulated in Person A's account at VASP C and were eventually transferred to a crypto wallet with an unknown address.

Source: APG

Case 19

Funds from Donation Fraud Converted into Crypto Assets – Philippines

Ms. H, a university student in a location assessed as high risk for TF, was under investigation for alleged involvement with a designated group in TF activities. Donations from various senders were channeled through electronic money provider X and MSB Z (in small amounts not exceeding PHP 2,000) over four months, totaling approximately PHP 92,000. Ms. H also received funds from various bank transfers amounting to approximately PHP 263,000 (around USD 4,703).

The collected funds appeared not to have been used for the advertised purposes but were instead used to purchase mobile phone credits and withdrawn by Ms. H. A portion of the funds was used to purchase fractional bitcoin, which was subsequently transferred to a crypto wallet with an unknown address.

The case was referred to the AMLC Secretariat by law enforcement, requesting a financial investigation into Ms. H and the bank accounts (with Ms. H as the account holder) that were posted on various social media accounts for donations for areas affected by a super typhoon, which may have been used to finance terrorism in the Philippines. The investigation is ongoing.

Source: APG

Case 20

Funds from Donation Fraud Converted into Crypto Assets – Philippines

In 2022, the AMLC received a report from a VASP revealing that an account holder had cashed out funds through a Money Service Business (MSB) and converted them into bitcoin. The funds were then sent to an unlabelled wallet address. Further analysis on blockchain platforms revealed that the bitcoin from that wallet address was eventually forwarded to another wallet address linked to transfers associated with or connected to terrorist organizations.
The matter has been referred to domestic law enforcement and international partners.

Source: APG

Case 21

Funds from Organized Crime Converted into Crypto Assets – Philippines

Mr. I and Mr. O posed as students from Jurisdiction X in the Philippines and enrolled in provincial colleges. Mr. R was a 29-year-old Filipino crypto trader who received fund transfers from nationals of Jurisdiction X suspected of involvement in hacking incidents. Based on transaction patterns at Bank Y, Mr. R and his associates from Jurisdiction X used a common law firm. Mr. I was recorded as having high-volume cash transactions at VASP C through his bank account at Bank Y, ranging from PHP 11,000 to PHP 2.2 million. Similarly, Mr. O also conducted high-volume cash transactions at VASP C.

Meanwhile, Mr. R conducted crypto-asset sales transactions (cash-outs) with VASP B amounting to PHP 5.5 million after Mr. I transferred funds to his account. Mr. R also sent two outward remittance transactions totaling PHP 1.8 million to a foreign PEP in Jurisdiction S, which is assessed as high risk for TF and hacking activities. Based on AMLC’s initial investigation, most of the proceeds from the hacking incident were believed to have ended up in unidentified crypto wallets, as planned, coordinated, and processed by Mr. I, Mr. O, and other anonymous members of the group involved in the hacking incident. In addition, Mr. I and Mr. O were reported to have recruited Filipinos across jurisdictions as money mules.

This information was forwarded to the National Bureau of Investigation on 29 September 2020.

A separate investigation revealed that Mr. R was a related party to a subject of interest in a drug-related case. This information was shared with law enforcement apparatus during a Target Intelligence Packaging workshop held in April 2021.

In a recent study entitled "Environmental Scanning: Cybercrime Threats and Actors", AMLC also identified Mr. I, Mr. O, and Mr. R as three of thirteen individuals identified as related parties in the hacking incident that occurred in June 2020. Several banks, pawnshops, and EMIs reported 801 suspicious transactions totaling PHP 162.3 million (approximately USD 2.9 million) involving thirteen individuals and one (1) corporate entity. The Environmental Scanning Study was disseminated to various AMLC stakeholders, including law enforcement apparatus, in November and December 2022.

Source: APG

Case 22

Suspected Violation of the Anti-Money Laundering Act by Platform G – Taiwan

A fraud network used online social media to promote investments in crypto asset Coin F issued by Platform G. To attract investors, the value of Coin F was claimed to be continuously increasing. The fraud network falsified fake investment return data on its website and reached internet users through communication software such as LINE. They initially requested small investments and made payments to generate profits in order to gain trust. They then persuaded investors to invest larger amounts of money. However, in January 2020, Platform G informed investors that their accounts had been frozen and all withdrawals suspended.

The fraud network consisted of Person A and his accomplices. They provided all of their financial account information to the fraud network to receive payments and transfer payments to victims' investment accounts, functioning as "money mules" for the network. They then used their crypto-asset wallets at multiple VASPs to purchase Tether (USDT) and other crypto assets, and subsequently transferred the crypto assets to cold wallets controlled by unknown persons. They also used third-party payment services to facilitate the transfer of proceeds of crime. The total amount of criminal proceeds was NTD 111,291,972 (approximately USD 3.45 million).

Source: APG

Case 23

Crypto-Asset Theft – Taiwan

Members of a criminal group applied for four accounts with a crypto-asset service provider, exploited a time-lag vulnerability that could not be updated in real time on the platform, and repeatedly conducted exchanges, sales, and withdrawals of crypto assets. From late 2020 to January 2021, the group took control of 300,000 USDT and 217 ETH with a market value exceeding NTD 25 million (approximately USD 775,000), and subsequently transferred the withdrawn crypto assets to accounts at other crypto-asset service providers to conceal the proceeds of crime.

Source: APG

Case 24

Illegal Online Casino Case – Thailand

Person A was investigated by the Thai Police and was found to operate an online gambling website. AMLO initiated a financial investigation into the illegal gambling activities, resulting in the seizure and freezing of various assets, including four supercars, one luxury car, bank accounts, and crypto-asset trading accounts. The total estimated value of the proceeds of crime exceeded THB 200 million (approximately USD 5.5 million). The case is currently undergoing legal proceedings.

Source: APG

Case 25

"Crypto Asset Expert" – Thailand

Person A, who claimed to be a "Crypto Asset Expert," defrauded numerous victims into investing in Bitcoin portfolios while using Facebook and game streaming platforms. Person A claimed that investors would receive high returns of approximately 30 percent on their investments and posted images of money transfers. Victims initially received returns; however, Person A later claimed that the bank was experiencing issues with fund transfers, causing delays in returns, and subsequently shut down his Facebook account and investment portfolio. Victims reported losses of approximately THB 22 billion (around USD 643,881,741) as a result of the scheme and filed complaints with the Royal Thai Police. Person A was arrested in January 2019.

Source: APG

INDONESIAN FINANCIAL TRANSACTION REPORTS AND ANALYSIS CENTER (INTRAC)

Jl. Ir. H. Juanda No. 35 Jakarta 10120 Indonesia
Phone: (+6221) 3850455, 3853922
Fax: (+6221) 3856809 – 3856826
Website: http://www.ppatk.go.id