Journal of Central Banking Law and Institutions, Vol. 1 No. 1, 2022, pp. 47 - 70
e-ISSN: 2809-9885
DOI: 10.21098/jcli.v1i1.7

FINANCIAL CRIME IN DIGITAL PAYMENTS

Jamal Wiwoho,[a] Dona Budi Kharisma,[b] Dwi Tjahja K. Wardhono[c]

[ab]Faculty of Law, Universitas Sebelas Maret, [c]Bank Indonesia Institute, Indonesia
e-mail: donabudikharisma@staff.uns.ac.id (corresponding author);
jamalwiwoho@staff.uns.ac.id; donny@bi.go.id

Submitted: 15 December 2021 - Last revised: 1 January 2022 - Accepted: 10 January 2022

Abstract

Digital payments are proliferating along with a massive and rapid digital transformation. However, the characteristics of transactions using digital payments, which are real-time, not face-to-face, and borderless create potential risks for financial crimes, including, Money Laundering and Funding Terrorism. The potential for abuse occurs in the registered and licensed digital payments sector and illegal digital payments that are not registered with the Bank Indonesia. Undoubtedly, this condition can threaten economic stability and financial system integrity. This article seeks to identify the potential for digital payment use for financial crime and construct a legal framework to prevent the misuse of FinTech for financial crime in Indonesia. This type of research is legal research. The research method used was a statutory comparative approach. The legal materials used were primary and secondary legal materials. The findings have been analysed using qualitative data analysis techniques. The results of the study show that several cases of terrorism financing have been proven to have used FinTech digital payments as a means of online funding. In this regard, to maintain the integrity of the financial system and strengthen the government's control functions, a comprehensive legal framework is needed through the establishment of Law on FinTech.

Keywords: *digital payments, financial crime, financial services*

I. INTRODUCTION

Financial technology (FinTech) is a technology that is being used for financial services to make transactions safer and more efficient.[1] The Financial Stability Board (FSB) defines FinTech as "technologically enabled financial innovation resulting in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services."[2]

---

[1] Jamal Wiwoho and Dona Budi Kharisma, *Isu-Isu Hukum Di Sektor FinTech* (Malang: Setara Press, 2021), 3-4.

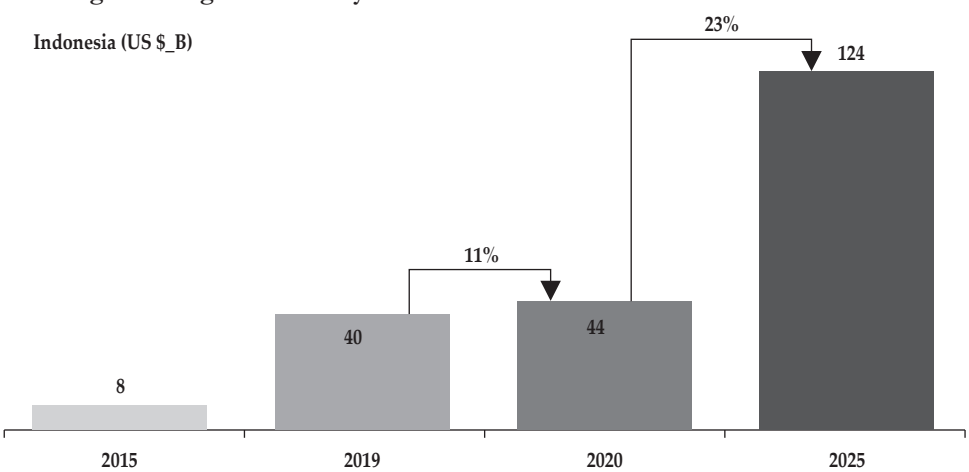
[2] Bank for International Settlement, *Basel Committee on Banking Supervision Consultative Document Sound Practices for the Management and Supervision of Operational Risk*, 2017; Financial Stability Board, "FSB Report Assesses FinTech Developments and Potential Financial Stability Implications," *Www.Fsb.Org*, 2019.

Bank Indonesia in Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Service Providers, defines FinTech as payment systems and financial service activities carried out by payment service providers who carry out funding source administration activities in the form of issuing electronic money in cooperation with third parties and using mobile-based technology and devices or other digital tools for the digital economy and financial inclusion.

Digital Payments are one type of FinTech that is developing in Indonesia. During the pandemic, digital transactions grew rapidly. It is in line with e-commerce transactions which also soared. In the Bank Indonesia Report Quarter I and II 2021, the value of e-commerce transactions increased by 63.36% (y-o-y) to IDR 186.75 trillion, Electronic Money (EU) also increased 41.01% (y-o-y) to IDR 132.03 trillion, and digital banking increased 39.39% (y-o-y) to IDR 17,901.76 trillion.[3] The increase in electronic money transactions indicates FinTech is increasingly in demand by the Indonesian people today.

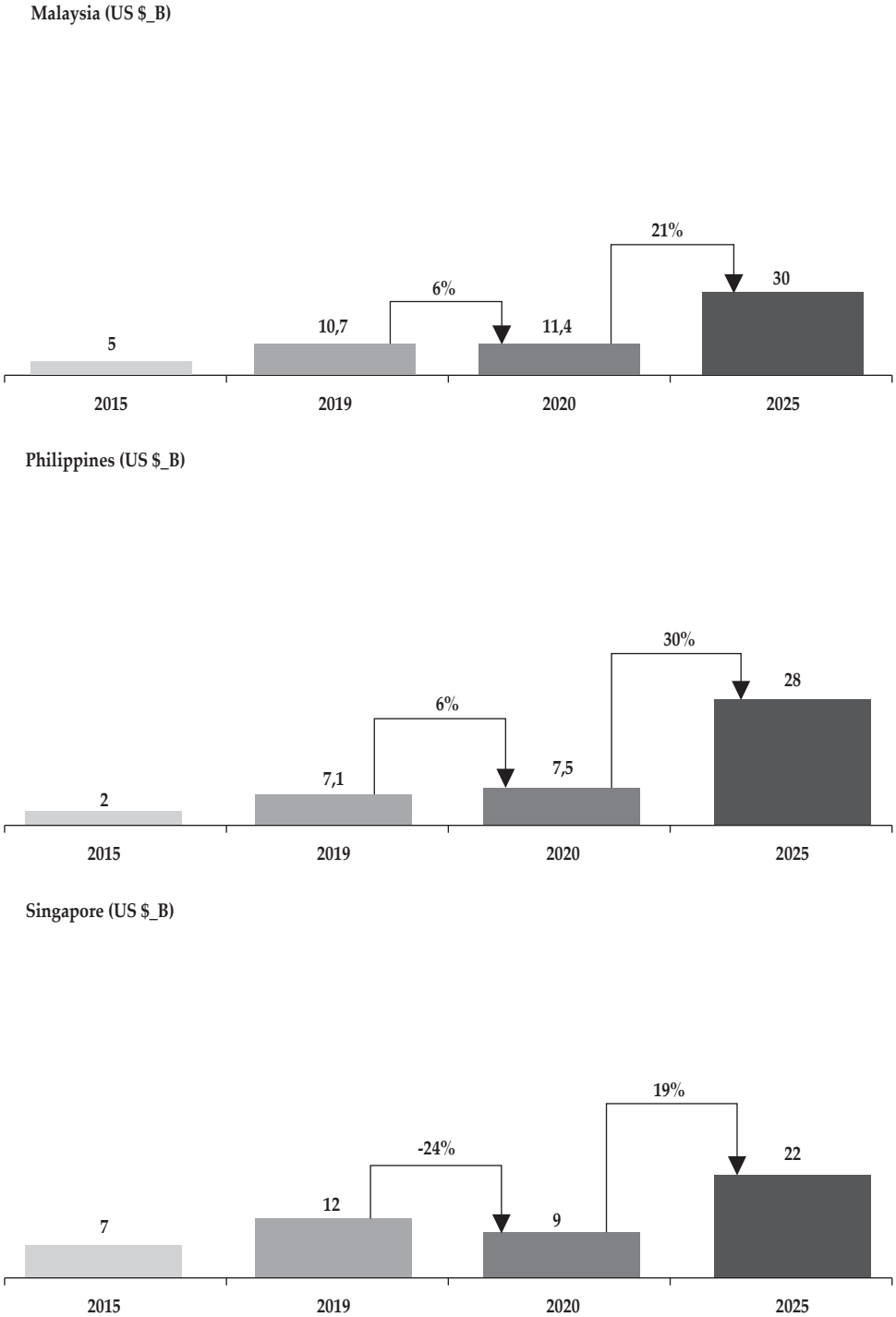
Based on reports from Google and Temasek in the e-conomy SEA 2020 report, the value of Indonesia's digital economy is the largest in the Southeast Asian region. In 2020, the valuation of Indonesia's digital economy reached US$44bn. Thailand only reached US $18bn, Vietnam reached US$14bn, Malaysia reached US$11.4bn, Singapore reached US$9bn and the Philippines reached US$7.5bn (Google et al., 2020) Figure 1.

Figure 1. Digital Economy Valuation Growth in Southeast Asian Countries



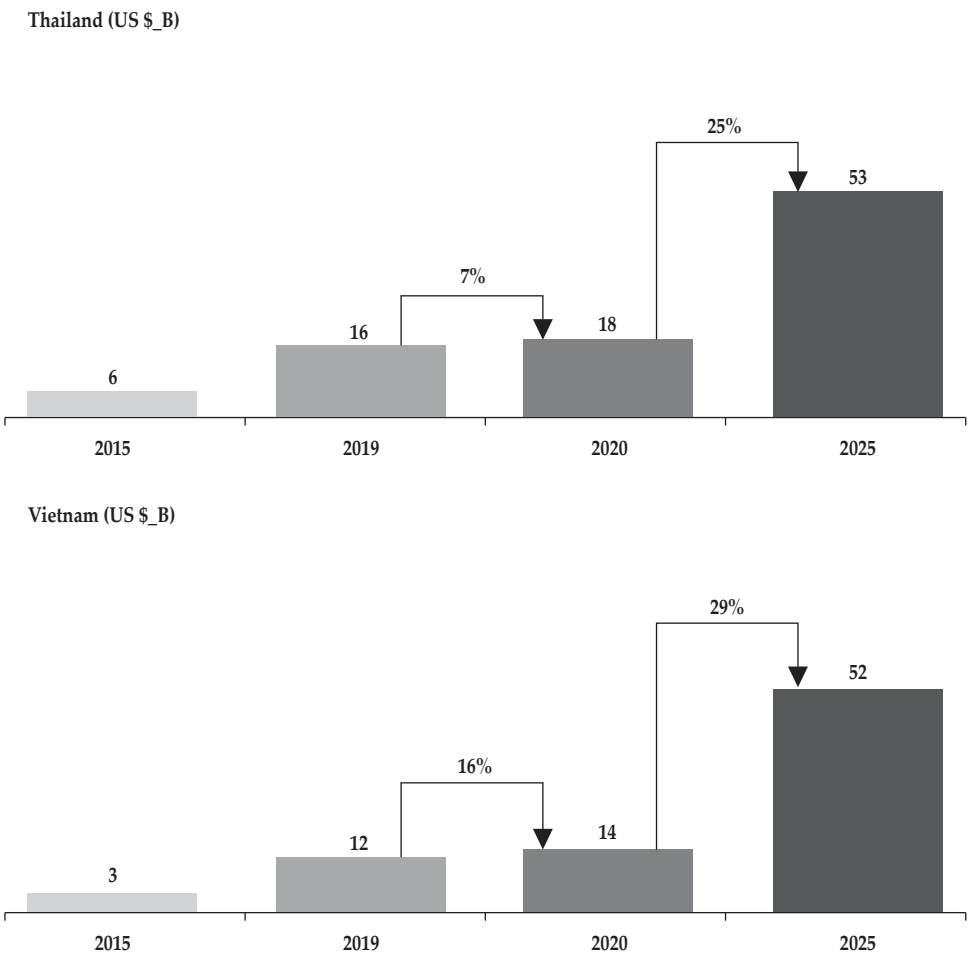
[3] Bank of Indonesia, "Laporan Kebijakan Moneter - Triwulan II Tahun 2021," 2021.

Figure 1. Digital Economy Valuation Growth in Southeast Asian Countries (Continued)



Source: Google, et al., 2020

Figure 1. Digital Economy Valuation Growth in Southeast Asian Countries (Continued)



Source: Google, et al., 2020

However, the massive use of digital payments has posed a severe challenge, namely the potential for financial crime. According to the International Monetary Fund (IMF), financial crimes are those that generally results in financial losses.[4] In current developments, financial crime includes fraud, electronic crime, money laundering, terrorist financing, bribery and corruption, market abuse and insider dealing, and breaches of information security.[5]

[4] International Monetary Fund, *Financial System Abuse, Financial Crime and Money Laundering* (Washington D. C.: the Monetary and Exchange Affairs and Policy Development and Review Departments IMF, 2001), 5-6.

[5] "What Is Financial Crime? | ICA," n.d.

There have been many empirical studies investigating this issue including that of Giorgio Merlonghi, which starts from the present and prospective characteristics of the payment means and moves on to briefly analyse the possible implications of their evolution in the fight against money laundering and the financing of terrorism. The analysis shows how factors that make innovative payment instruments desirable may, at the same time, represent elements of weakness in the prevention of financial crime.[6]

In addition, research conducted by Angela Irwin *et al.* identified the potential for financial crime in virtual environments. This research has found that money laundering and terrorism financing can take place inside virtual environments. Virtual money laundering and terrorism financing benefit from anonymity, low likelihood of detection, and the absence of many risks associated with real-world money laundering and terrorism financing activity. However, this comes at the cost of ease, time, and in some cases, the amount of funds laundered. Large sums (millions of dollars) can be laundered in virtual environments, but this exponentially increases the level of effort involved in setting up accounts and placing, layering, and aggregating funds.[7]

Similarly, Teichmann has drawn the same conclusions from his research. Even though banks have implemented strict controls, they often do not pay the same attention to terrorism financing as they do to money laundering. In one recent case, refugees and "tourists" may have been involved in terrorism financing. When it comes to transferring larger amounts of money, terrorists do not necessarily act in their own name, but rather hire "straw men," through whom, some terrorists have proceeded to set up legitimate front companies in Turkey. Terrorists can explain why funds need to be transferred from Europe to Turkey through "charitable contributions" and transfers of large sums can also be facilitated by sham lawsuits.[8]

In a different vein, J. Jagtiani found that the regulations are important for consumer protection and to maintain financial stability while at the same time

---

[6] Giorgio Merlonghi, "Fighting Financial Crime in the Age of Electronic Money: Opportunities and Limitations," *Journal of Money Laundering Control* 13, no. 3 (2010): 202–14, https://doi.org/10.1108/13685201011057118.

[7] Angela S.M. Irwin et al., "Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study," *Journal of Money Laundering Control* 17, no. 1 (2014): 50–75, https://doi.org/10.1108/JMLC-06-2013-0019.

[8] Fabian Maximilian Johannes Teichmann, "Financing of Terrorism through the Banking System," *Journal of Money Laundering Control* 22, no. 2 (2019): 188–94, https://doi.org/10.1108/JMLC-07-2017-0026; Fabian Maximilian Teichmann, "Recent Trends in Money Laundering and Terrorism Financing," *Journal of Financial Regulation and Compliance* 27, no. 1 (2019): 2–12, https://doi.org/10.1108/JFRC-03-2018-0042.

creating an environment for safe FinTech innovations.[9] In addition, there was a study conducted by D.W. Arner et al,[10] S. Saksonova and I. Kuzmina-Merlino[11] and Philip Treleaven[12] who concluded that the formation of regulations on FinTech is very important.

However, based on these studies, there has been no research to identify various factors that encourage the abuse of digital payments for financial crime along with constructing a legal framework to prevent the misuse of digital payments for financial crime in Indonesia. Based on the above background, this article has two (2) problem formulations: the potential of digital payments in facilitating financial crime and establishment of Law on FinTech as a legal framework for preventing digital payments from facilitating financial crime.

II. FINTECH AND FINANCIAL CRIME

II.A. Definition of Fintech

FinTech is an example of successful digital transformation. In the economic context, digital transformation is defined as a sustainable, company-level transformation via revised or newly created business operations and business models achieved through value-added digitisation initiatives, ultimately resulting in improved profitability."[13] Thus, digital transformation means the pervasive use of technology to improve business profitability.

The definition of FinTech is any innovative ideas that improve financial service processes through technological solutions according to different business situations, with the possibility of ideas leading to new business models or even new businesses.[14]

The Financial Stability Board (the FSB) defines FinTech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on

---

[9] Julapa Jagtiani and Kose, John, "FinTech: The Impact on Consumers and Regulatory Responses," *Journal of Economics and Business* 100, no. November 2018 (2018): 1–6, https://doi.org/10.1016/j.jeconbus.2018.11.002.

[10] Douglas W. Arner, Jànos Barberis, and Ross P. Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation," *Northwestern Journal of International Law and Business* 37, no. 3 (2017): 373–415.

[11] Svetlana Saksonova and Irina Kuzmina-Merlino, "FinTech as Financial Innovation - The Possibilities and Problems of Implementation," *European Research Studies Journal* 20, no. 3 (2017): 961–73, https://doi.org/10.35808/ersj/757.

[12] Philip Treleaven, "Financial Regulation of FinTech," *Journal of Financial Perspectives* 3, no. 3 (2015): 114–21.

[13] Daniel R A Schallmo and Christopher A Williams, *Digitalization of Your Business Model*, 2018.

[14] Kelvin Leong, "FinTech (Financial Technology): What Is It and How to Use Technologies to Create Business Value in FinTech Way?," *International Journal of Innovation, Management and Technology* 9, no. 2 (2018): 74–78, https://doi.org/10.18178/ijimt.2018.9.2.791.

financial markets and institutions and the provision of financial services."[15] The FSB defines FinTech more broadly to include various innovations in financial services that use technology regardless of the type, size, and arrangement of the FinTech itself. The expansive definition is useful for assessing and anticipating the rapid developments in the financial system and financial institutions, the risks and opportunities associated with FinTech.

Based on these definitions, there are two facets of FinTech, namely "technological" and "financial." The term "technology" refers to the use of new technologies and innovative business models that change existing traditional patterns or habits. New technology includes cognitive computing, machine learning, artificial intelligence, blockchain, and distributed ledger technologies through the internet network.

Then, the term "financial" refers to financial services in the banking industry, finance industry, investment, insurance industry, and other financial industries. There are several kinds of financial services, including digital payments, e-wallets, electronic money, equity crowdfunding, insurtech, and various other financial services. Thus, FinTech can be defined as the use of technology in financial service innovation through the Internet.

II.B. Benefits and Types of FinTech

The presence of FinTech provides substantial benefits for financial stability, including:[16]

1. Decentralisation and diversification. FinTech may lead to greater decentralisation and diversification in several areas. In lending, technological advances, such as big data processing and automation of loan originations, have reduced barriers to entry.
2. Efficiency. Innovations in financial services have the potential to lead to greater efficiencies. Adoption of productivity-enhancing technologies, such as robo-advice, RegTech or applications of technology that streamline back-office functions, could strengthen business models of incumbent financial institutions. Machine learning and AI could facilitate improvements in decision-making processes, by improving the models that financial institutions and investors use.
3. Transparency. Increased and better uses of data have the potential to reduce information asymmetries in many areas of FinTech. Better quality adata could also allow for the creation of smart contracts that more accurately target specific risks. FinTech lending and equity crowdfunding

[15] Financial Stability Board, "Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention," *Financial Stability Board*, no. June (2017): 1–61.

[16] Financial Stability Board.

could further complement markets for both households and businesses (e.g., SMEs).

4. Access to, and convenience of, financial services. Clearly, the potential for improved access to a range of financial services across all the economic functions is the most needed in regions where there are currently a large unbanked population, and where the financial system is in early stages of development. Mobile banking allows consumers to quickly obtain credit and make purchases quickly and efficiently. Innovations such as digital identity and DLT-based applications could improve the quality and accessibility of, or financial services accessibility for, end-users.

The types of FinTech that are developing in Indonesia include:[17]

1. Digital Payments. FinTech digital payments provide services in the form of online transaction payments which are more practical, fast, and cheap. These service providers are generally in the form of a virtual wallets, commonly called e-wallets, which are equipped with various features to facilitate online transactions between consumers and business owners or between business actors (B2B).
2. Financing and Investments. This type of FinTech provides crowdfunding and peer-to-peer lending (P2P Lending) services. FinTech crowdfunding generally raises funds for a profit or non-profit project or social fundraising. On the other hand, FinTech P2P lending usually facilitates parties who need to borrow funds with parties who want to invest by providing loans.
3. Account Aggregators. FinTech account aggregators offer services that can accommodate all transactions through a single platform. Platform users are given the convenience of verifying transactions because the process is abbreviated. This type of FinTech also provides financial reporting services where information is obtained from banking accounts registered on the platform.
4. Information and Feeder Sites. This type of FinTech provides services regarding the information needed by potential consumers who want financial products or services. The information provided can be in the form of information, such as credit cards, interest rates, mutual funds, insurance premiums, and so on. In general, this type of FinTech also provides services for making comparisons that are tailored to the needs of consumers. These companies also provide registration services for the purchase of financial sector products or services, such as purchasing insurance premiums.

[17] OJK, "Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Perlindungan Konsumen Pada FinTech," *Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan*, 2017, 1-86.

5. Personal Finance. This type of FinTech through its platform helps consumers from making good financial reports to choosing wise fund processing. The mechanism commonly used starts from notification of consumer financial information on the FinTech company's platform. Then the FinTech company will process, assess information, and provide advice as the output of a company's services.

II.C. Definition and Types of Financial Crime

The International Monetary Fund (IMF) defines financial crime as a crime that generally results in financial loss.[18] Meanwhile, Section 6(3) of the UK's Financial Services and Markets Act 2000 (FSMA 2000), defines financial crime as any offence involving fraud or dishonesty, misconduct in or misuse of information relating to a financial market, or handling criminal proceeds.

The UK's Financial Services Authority (FSA) also provides a definition of financial crime that has similar practical implications, stating it to be any offence involving money laundering, fraud or dishonesty, or market abuse.[19] That means that according to English Law, financial crime is all financial crimes in the form of fraud, fraud, and/or misuse of financial-related information. In comparison, the financial crime itself has practical implications for handling the proceeds of financial crimes, any crime involving money laundering, fraud or dishonesty, or abuse of markets in finance.

In reference to these definitions, financial crime can be in the form of first, the crime of theft, fraud, or fraud that aims to gain profit from other people in the financial sector. For example: account theft, ATM skimming, credit card fraud, and fake sweepstakes. Second, financial crime can appear as financial crimes to hide, protect or obscure the origin of assets obtained from the proceeds of criminal acts. This includes money laundering. The financing of terrorism is also included in the category of financial crime.

However, the primary forms financial crime for purposes of this article are money laundering and terrorism financing.[20] Meanwhile, according to the International Compliance Association (ICA), recently, the types of financial crime have come to include fraud, electronic crime, money laundering,

---

[18] International Monetary Fund.

[19] The Chartered Institute for Securities & Investment (CISI), The Background and Nature of Financial Crime (London: CISI, 2nd), 3-4.

[20] Irwin et al., "Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study"; Esman Kurum, "RegTech Solutions and AML Compliance: What Future for Financial Crime?," *Journal of Financial Crime*, 2020, https://doi.org/10.1108/JFC-04-2020-0051; Angela Samantha Maitland Irwin, Kim Kwang Raymond Choo, and Lin Liu, "An Analysis of Money Laundering and Terrorism Financing Typologies," *Journal of Money Laundering Control* 15, no. 1 (2011): 85–111, https://doi.org/10.1108/13685201211194745.

terrorist financing, bribery and corruption, market abuse and insider dealing, and breaches of information security.[21]

In Indonesia, financial crime falls under Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering (Law on Money Laundering) and Law No. 9 of 2013 on Prevention and Eradication Terrorism Financing Crimes (Law on Terrorism Financing).

III. REGULATORY FRAMEWORK IN INDONESIA FOR FINTECH DIGITAL PAYMENTS

III.A. Statutory framework for FinTech Digital Payments

Indonesia does not yet have a law that specifically regulates FinTech. However, laws and regulations governing financial services, information technology and electronic transactions can be the legal basis for implementing FinTech digital payments. These regulations include:

1. Law No. 8 of 1999 on Consumer Protection;
2. Law No. 23 of 1999 on Bank Indonesia, amended by Law No. 6 of 2009;
3. Law No. 11 of 2008 on Electronic Information and Transactions, amended in Law No. 19 of 2016;
4. Law No. 3 of 2011 on Funds Transfers;
5. Law No. 21 of 2011 on the Indonesia Financial Services Authority (OJK);
6. Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (PTSE); and
7. Government Regulation No. 80 of 2019 on Electronic Commerce.

In addition, there are several Bank Indonesia regulations that of FinTech digital payments, including:

Table 1.
Technical Regulations of FinTech Digital Payments

No	Bank Indonesia Regulations (PBI)
1	Bank Indonesia Regulation No. 21/5/PBI/2019 on Operators of Transaction Implementation Facilities in the Money Market and Foreign Exchange Market.
2	Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Service Providers.
3	Bank Indonesia Regulation No. 23/7/PBI/2021 on Payment System Infrastructure Operators.

III.B. FinTech Digital Payments Regulation

The use of FinTech digital payments is closely related to the financial system. FinTech digital payments pose potential risks that can disrupt the financial system

[21] International Compliance Association (ICA).

and therefore needs to be properly mitigated. Bank Indonesia, as mandated in Act Number 23/1999 on Bank Indonesia, amended in Law No. 6 of 2009, is mandated with maintaining monetary stability, financial system stability, and the payment system. Therefore, Bank Indonesia as a national payment gateway has legal standing to regulate and supervise the implementation of the Sharia FinTech industry, especially FinTech that organises payment transaction processing or payment service providers.

Payment service providers are banks or institutions other than banks that provide services to facilitate payment transactions to users. Payment service providers carry out activities that include:

1. providing information on sources of funds which includes providing information on sources of funds for initiation of payments based on the approval of service users;
2. initiating payments and/or acquiring services which include forwarding of payment transactions;
3. administrating sources of funds include administration of source of funds account and execution of authorisation of payment transactions;
4. remittance service is an activity of organising fund transfers in the form of acceptance and execution of fund transfer orders whose sources of funds are not from accounts administered by remittance service providers.

FinTech that provides payment services is called FinTech digital payments which includes payment processing, money transfer mobile payments, and digital wallets. FinTech payments provide digital payments that are fast, safe, do not contain usury, and cooperate with banks so that the accumulated balance is stored in the bank.

The role of Bank Indonesia in regulating and supervising FinTech digital payments includes:

1. Licensing;
   FinTech that provides payment services must have authorisation from Bank Indonesia. Permits are categorised according to the activities of FinTech payment service providers, which consist of:
   a. permit category one includes activities:
      1) administration of funding sources;
      2) provision of information on sources of funds;
      3) payment initiation and/or acquiring services; and
      4) remittance services;
   b. category two permits include activities:
      1) providing information on sources of funds; and
      2) payment initiation and/or acquiring services;

c. category three permits include activities:
   1) remittance services; and/or
   2) others as determined by Bank Indonesia.

Some of the permit requirements that must be met include the following aspects:

a. Institutions covering entity legality, ownership, control, and management.
b. capital and finance that includes minimum paid-up capital requirements, feasibility analysis, and business projections.
c. risk management, which includes legal risk, operational risk, and liquidity risk.
d. information system capabilities which include information system security control procedures, fraud management system, information system audit and security testing, and the level of capability and availability of information systems.

2. Trial;

Bank Indonesia provides an incubator aimed at encouraging technological innovation and monitoring and detecting the opportunities and risks of technological innovation on the development of the digital economy and financial ecosystem as well as the implementation of payment systems. Facilitation of experimental instruments for the development of Payment System technology innovations, including:

a. An innovation lab, namely the development of innovations that have not been used or have been used in the payment system industry on a limited basis;
b. a regulatory sandbox, namely innovation on payment system policies or provisions; and
c. an industrial sandbox, namely an innovation that has been used in the payment system industry and needs to be encouraged to become widely used.

The results of the trial can be deemed successful or unsuccessful. If the trial is declared successful, and the product, activity, service, or business model is included in the category of payment system operation, the FinTech operator is prohibited from marketing the product, activity, service, and business model being tested before obtaining a permit and/or approval in accordance with Bank Indonesia regulations. regarding the payment system.

However, if the test results are declared unsuccessful and the product, activity, service, and business model are included in the category of payment system operations, in which the FinTech operator is prohibited

from marketing the product and/or service or using the technology and/or business model being tested.

3. Supervision

   Bank Indonesia supervises the implementation of payment systems using a risk-based and/or compliance approach. Supervision is carried out with the aim of creating payment systems that are fast, easy, cheap, safe, and reliable, but still encourage innovation and pays attention to international standards and practices.

   The object of supervision includes risk exposure (including compliance with the provisions of laws and regulations), implementation of governance and risk management, and other aspects as determined by Bank Indonesia. The mechanism for monitoring the implementation of the payment system is carried out through:

   a. Indirect supervision.

      Indirect supervision is carried out through monitoring, identification, and/or assessment through analysis of reports, data, and information obtained by the Bank Indonesia.

   b. Direct supervision.

      Direct supervision is carried out through periodic inspections at any time, either face-to-face or other mechanisms established by Bank Indonesia. Inspections are carried out of documents, infrastructure, information systems, and other aspects used by PJP.

   Based on the results of supervision, Bank Indonesia carries out follow-up supervision in the form of:

   a. Directing PJP to:
      1) act or refrain from action;
      2) limit activities or operations; and/or
      3) temporarily cease, in part or in whole, or all the activities including the implementation of the cooperation; and/or

   Revoking the permit and/or approval that had been granted.

IV. POTENTIAL ABUSE OF DIGITAL PAYMENTS FOR FACILITATION OF FINANCIAL CRIME

The Indonesian Financial Transaction Reports and Analysis Center (PPATK) states that suspicious financial transaction reports have increased during the Covid-19 pandemic. The report covers various crimes such as corruption, fraud, online gambling, tax crimes, and manipulation of capital markets, where

the perpetrators take advantage of the pandemic conditions to perpetrate these criminal acts.[22]

This situation, of course, requires serious attention from the government and Bank Indonesia. In addition to supporting the application of the precautionary principle to protect payment system operators and users of payment system services from various risks that may arise, these conditions can undoubtedly threaten economic stability and the financial system's integrity.

In the current era of digital transformation, digital payments are vulnerable to abuse. The characteristics of digital payment transactions that are real-time, not face-to-face, and borderless pose potential risks for financial crimes such as money laundering and terrorism financing. Through digital payments, the transaction and transfer mechanism do not pass through the Central Bank or other formal institutions, eluding safeguards and making the risk of money laundering and terrorism financing challenging to avoid.[23]

The pseudonymity of the transaction mechanism allows the perpetrator of the transaction to be difficult to be identify. Transactions are augmented and easier to move, even abroad. Therefore, it is difficult to freeze or confiscate fund-related crimes.[24] That is a challenge as well as a risk of using digital payments in Indonesia.

One example is the financing of terrorism through digital payments. Take the case of Bahrun Naim, one of the terrorist bombers in Indonesia, who used several online payment accounts, PayPal and Bitcoin, for terrorism financing and many other cases.[25] Five terrorism networks use digital payments to raise funds through campaigns on social media with the mode of humanitarian assistance for natural disasters, victims of the Palestinian and Syrian conflicts, residents exposed to Covid-19 under the guise of orphanage assistance. That five terrorist networks are the Negara Islam Indonesia (NII), Jamaah Islamiyah (JI), Majelis Mujahidin Indonesia (MMI), Jamaah Ansharut Tauhid (JAT), and Jamaah Ansharut Khilafah (JAK).[26]

---

[22] Dian Ediana Rae, "Profiling Kejahatan dan Kerentanan Pencucian Uang serta Pendanaan Terorisme sebagai Dampak Krisis Covid-19", Jakarta, 19 August 2021. Pusat Pelaporan Analisis dan Transaksi Keuangan (PPATK), "Perbankan Harus Sigap dan Waspada Selama Pandemik Covid-19", 21 August 2021, https://www.ppatk.go.id/siaran_pers/read/1073/siaran-pers-kepala-ppatk-perbankan-harus-sigap-dan-waspada-selama-pandemik-covid-19.html.

[23] Artie W. Ng and Benny K.B. Kwok, "Emergence of FinTech and Cybersecurity in a Global Financial Centre: Strategic Approach by a Regulator," *Journal of Financial Regulation and Compliance* 25, no. 4 (2017): 422–34, https://doi.org/10.1108/JFRC-01-2017-0013.

[24] Daniel Dupuis and Kimberly Gleason, "Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic," *Journal of Financial Crime*, 2020, https://doi.org/10.1108/JFC-06-2020-0113.

[25] Sindo News, "Pendanaan Terorisme Kian Canggih, Berubah Seiring Perkembangan Teknologi," 2020.

[26] Koran Bisnis, "Lima Jaringan Teroris Manfaatkan FinTech, DPR_ Lacak! - Kabar24 Bisnis," n.d.

The mode of money laundering has also changed, namely by using digital payments to make it more difficult to track. It is not often that perpetrators use Bitcoin to obscure the results of criminal acts.[27] The latest is The Attorney General of the Republic of Indonesia (Kejaksaan Agung) finding that three suspects in the PT ASABRI corruption case hid the proceeds of their crimes through cryptocurrency transaction. The head of the Indonesian Financial Transaction Reports and Analysis Center (PPATK) Dian Ediana Rae said that the concealment of the proceeds of crime through cryptocurrency or bitcoin transactions identified in Indonesia since 2015.[28]

FinTech abuse targets not only licensed FinTech also illegal FinTech. The Investment Alert Task Force noted that Illegal FinTech Lending was increasingly prevalent during the Covid-19 pandemic. On April 2020 data, for example, 81 illegal FinTech lending entities potentially harmed the community.[29] This condition means that FinTech will be very vulnerable to being used as a means of the financial crime if the government's control function does not work well.

V. ESTABLISHMENT OF A LEGAL FRAMEWORK FOR DIGITAL PAYMENTS PREVENTION FOR FINANCIAL CRIME

Indonesia currently does not have a law that explicitly regulates the FinTech industry, in contrast to other financial industries which are specifically regulated. The capital market industry is regulated in Law No. 8 of 1995; the banking industry is regulated in Law No. 7 of 1992 as regulated in Law No. 10 of 1998; the insurance industry is regulated in Law No. 40 of 2014. Other related Law such as the Law on Bank Indonesia, Law on Banking, and the Law on OJK have also not touched the FinTech industry.[30]

Regarding FinTech, it is regulated in Bank Indonesia Regulations (PBI) such as PBI No. 23/6/PBI/2021 on payment service providers. In addition, a FinTech faces regulations that are not related to the payment system in the Financial Services Authority Regulation (POJK). That means that in the

---

[27] Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime*, 2021, https://doi.org/10.1108/JFC-09-2021-0193.

[28] Koran Kompas, "Tersangka Kasus Asabri Cuci Uang Lewat Bitcoin, PPATK_ Modus Baru TPPU Halaman All - Kompas," n.d.

[29] "Pandemi Covid-19, OJK_ Investasi Ilegal Marak Bermunculan - Bisnis Tempo," n.d.

[30] Dona Budi Kharisma, "Mengagas Pembentukan Lembaga Alternatif Penyelesaian Sengketa (LAPS) Di Sektor Industri *Financial Tecnology* (*FinTech*)", Buletin Hukum Kebanksentralan, Vol 17, 2, Juli - Desember (2020), 158-159.

context of the Act, the regulation regarding FinTech is in a legal vacuum, which can lead to legal uncertainty, even chaos.[31]

The new FinTech regulations regulated in the PBI and POJK have weak administrative powers compared to regulations in the form of statutes. This is due to several things, including:[32]

Table 2.
PBI and POJK Weaknesses

No	Legal Aspect	PBI	Legal Consequence
1.	Legal Substance	Lacks criminal sanctions	PBI is not regulations at the level of a statute so the substances regulated cannot contain criminal sanctions. On the one hand, the misuse of FinTech for financial crime and the rise of illegal FinTech is a criminal act.
2.	Formal procedures in the formation of Laws and regulations.	No formal procedures for the formation of laws and regulations. The involvement of political infrastructure, preparation of academic texts, public hearings, and public examinations are formal procedures for forming the legislation.	Forming regulations that do not go through formal procedures results in a lack of public participation, comprehensive arrangements, and less transparent and democratic regulations.
3.	Type and character of regulation.	Secondary legislation or implementing regulations of a technical characteristic.	Consider the implementing regulations are technical, all basic legal norms not regulated. Fundamental norms like the outline of things that should finish (*obligattere*), which prohibit from being done, or finish (*prohibere*), and which are allowed to finish (*permittere*) are not yet regulated.

Several countries can be used for comparison with Indonesian FinTech regulations, including Mexico, Singapore, America, and Liechtenstein. Mexico has the Mexican FinTech Act enacted in 2018. That Act established FinTech licensing and supervision, business activities, and risk mitigation in the Mexican financial system by limiting the types of FinTech and crafting the FinTech licensing process.[33]

[31] Yudho Taruno Muryanto, Dona Budi Kharisma, and Anjar Sri Ciptorukmi Nugraheni, "Prospects and Challenges of Islamic FinTech in Indonesia: A Legal Viewpoint," *International Journal of Law and Management*, 2021, https://doi.org/10.1108/IJLMA-07-2021-0162.

[32] Dona Budi Kharisma, "Urgency of Financial Technology (FinTech) Laws in Indonesia," *International Journal of Law and Management* 63, no. 3 (2020): 320–31, https://doi.org/10.1108/IJLMA-08-2020-0233.

[33] Frick, T.A (Ed), Law Review, "Financial Technology Financial Technology Law Review," 2021.

We can further observe through comparison with regulations on FinTech in Singapore. In Singapore, there are several Act in which there are regulations regarding FinTech. For example, the Payment Services Act 2019 (PS Act) was applicable on January 14, 2019. The PS Act regulates payment services and increases the scope of regulated payment activities to cover digital payment token services and other innovations. The PS Act serves to build a simple, secure, and accessible payment ecosystem. These ventures include money laundering and terrorism financing risks, protection for consumers and providers, and technology risks.[34]

Moreover, The United States has the Act governing FinTech. One aspect is the Jumpstart Our Business Startups Act (JOBS Act), enacted to support start-up businesses, especially those in the FinTech sector. In addition to supporting start-ups, the JOBS Act also aims to protect consumers, investors, mitigate risks and prevent money laundering and terrorism financing.[35] Similarly, Liechtenstein has a Blockchain Act that functions effectively in law enforcement of financial crime in the FinTech sector.[36]

Regulations on FinTech in these countries stem from concerns about several things, including fraud, investment fraud, securities of cryptocurrencies, systemic risk regulation, taxation, money laundering, and terrorism financing.[37] Therefore, an Indonesian Act on FinTech is essential. The government and authorities need to have legal standing to supervise and control FinTech businesses strictly.

There are two main functions of the Act on FinTech. First, the FinTech Act functions as a legal framework in regulating and supervising the FinTech industry. The use of FinTech in all financial services, both in the banking sector, capital markets, and non-bank financial services sector such as insurance, pension funds, financial institutions, and other financial services institutions, of course, requires additional regulation and supervision. Therefore, a strong FinTech Act can act as a legal basis for regulating licenses to establish FinTech entities, FinTech business activities, the fitness level of FinTech entities, including FinTech governance, the principle of knowing customers, and

---

[34] David Kuo Chuen Lee and Linda Low, "FinTech in Singapore," *Inclusive FinTech*, 2018, 307–79, https://doi.org/10.1142/9789813238640_0008.

[35] Michael Nonaka et al., "FinTech in the United States - Regulatory Compliance," *Thomson Reuters Practical Law*, 2019, 1–17.

[36] Fabian Maximilian Johannes Teichmann and Marie Christin Falker, "Money Laundering via Cryptocurrencies – Potential Solutions from Liechtenstein," *Journal of Money Laundering Control*, no. January (2020), https://doi.org/10.1108/JMLC-04-2020-0041.

[37] Mohammed Ahmad Naheem, "Regulating Virtual Currencies – the Challenges of Applying Fiat Currency Laws to Digital Technology Services," *Journal of Financial Crime* 25, no. 2 (2018): 562–75, https://doi.org/10.1108/JFC-08-2016-0055.

anti-money laundering and preventing the financing of terrorism and other financial crimes.

Second, the FinTech Act can function to mitigate the risk of various potential risks such as system failure, financial crime, misinformation, error transactions, data security, implementation of 'Know Your Customer (KYC) principles,' prohibition of usurious interest rates, exoneration clauses, and how to handle complaints from customer service users. If the potential for high risk does not mitigate correctly, it can affect monetary stability, consumer protection, and the FinTech industry's growth.[38]

There are five aspects of FinTech supervision that need to be regulated in the FinTech Act, namely: (1) customer protection; (2) anti-money laundering and counter financing terrorism; (3) risk management; (4) data protection and security; and (5) individual empowerment.[39]

In FinTech supervision, the first aspect is customer protection. Five principles of customer protection must be applied, namely transparency, fair treatment, reliability, confidentially and security of consumer data/information, and handling of complaints and settlement of consumer disputes in simple, fast manner, and at reasonable cost.

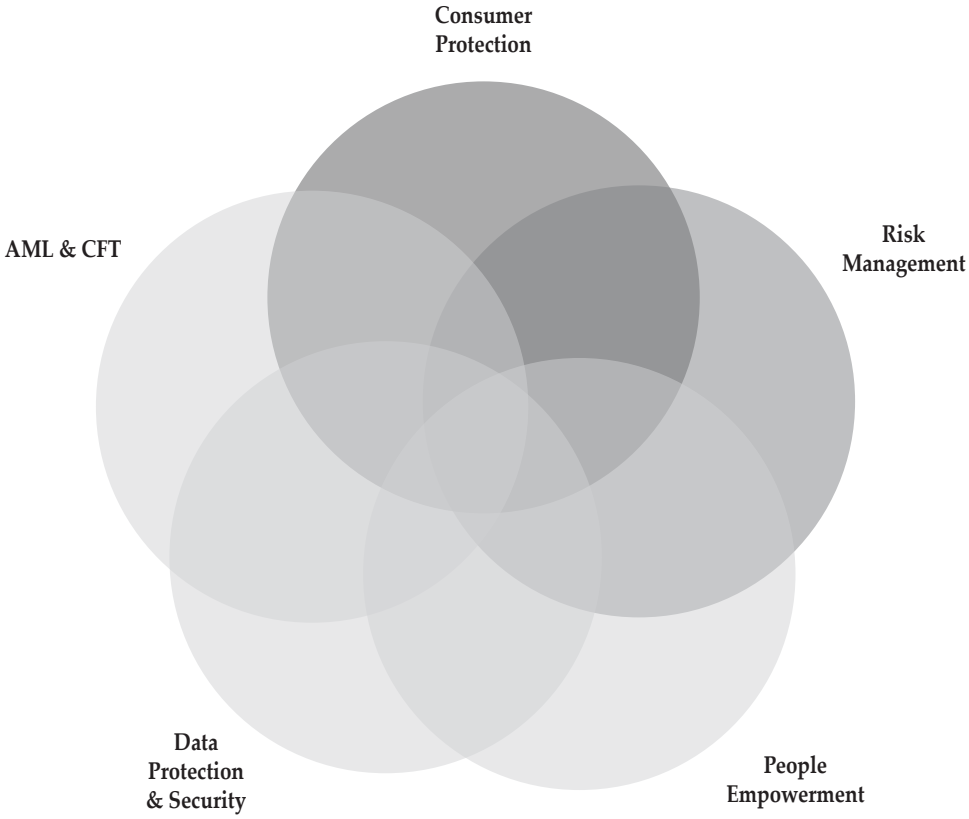
Second, is legislation for anti-money laundering and counter-financing terrorism. Funds must not be misused or collected out of one's ill intentions. Third, the risk management approach. This approach includes mitigation of strategic risk, systemic operational risk, individual operational risk, the risk of money laundering & financing of terrorism, the protection of consumer data, risk of using third party services; cyber risks; and liquidity risk.

Fourth, the data protection and security aspects. Data should not be misused, and information technology systems should be resistant to cyber-attacks. Five, people empowerment with provides the greatest benefits for economy and society.

[38] Kharisma, "Urgency of Financial Technology (FinTech) Laws in Indonesia."

[39] Wimboh Santoso, "FinTech and The Future of Finance", Surakarta Indonesia, 12 March 2020.

Figure 2. Five Approach FinTech Supervision



In the context of substance, several vital substances that need to regulate in the FinTech Act in the future include:

Table 3.
Act on FinTech Substance

No.	Act on FinTech substance	Legal reasoning
1	Criminal Sanctions	The misuse of FinTech for facilitation of financial crime and the increasing number of illegal FinTech practices, fraud, usury, and the use of personal data without the owner's permission are criminal acts. Therefore, to strengthen the relevant authorities in handling FinTech cases and improve customer protection, the material on the content of criminal sanctions needs to be included.

Table 3.
Act on FinTech Substance (Continued)

No.	Act on FinTech substance	Legal reasoning
2	Classification of authority, coordination, and synergy between authorities (BI and OJK) in licensing and supervision of FinTech.	There is still overlapping licensing and supervision of the FinTech industry because the authority is shared by two institutions, namely BI and OJK. Explicit arrangements regarding authority and coordination between authorities expect to improve the performance of each authority. Cases like Century Bank will not be repeated in the FinTech sector if each authority has apparent authority and boundaries.
3	Prevention and handling of digital financial system crises	Mechanisms to prevent and handle FinTech problems and digital financial system crises that can have a systemic impact are also necessary to regulate. Substances that need to be regulated include (i) coordinating the monitoring and maintenance of the stability of the digital finance financial system, (ii) handling digital financial system crises, and (iii) handling systemic problems with FinTech operators, both under normal conditions and in digital financial system crises.
4	Consumer dispute resolution mechanisms and FinTech Alternative Consumer Dispute Resolution Institutions	Consumer protection is the leading motivator in the financial services industry. Therefore, it is essential to consider creating a consumer dispute resolution mechanism in the FinTech sector. In addition, the establishment of an Alternative Consumer Dispute Resolution Institution in the FinTech sector, as already exists in other financial industry sectors, also needs to be considered by legislators.

VI. CONCLUDING REMARKS

The use of digital payments in Indonesia faces serious challenges, one of which is the misuse of digital payments for facilitation of financial crime. Several cases of terrorism financing have been proven to use digital payments as a means of online funding. Perpetrators of criminal acts of corruption have also been proven to use digital payments to hide the proceeds of their crimes (money laundering). The characteristics of transactions in digital payments that are real-time, non-face-to-face meetings, and borderless make digital payments an emerging threat in Indonesia.

A comprehensive legal framework on FinTech needs to develop to maintain the integrity of digital payments and strengthen the government's control function. There are two main functions of the FinTech Act: first as a legal framework in regulating and supervising the FinTech industry; and secondly, as a risk mitigation tool for various potential risks such as system failure, financial crime, misinformation, error transactions, data security, implementation of "Know Your Customer" (KYC) principles, exoneration clauses, and dispute resolution mechanisms between service providers and users.

REFERENCES

Arner, Douglas W., Jànos Barberis, and Ross P. Buckley, "FinTech, RegTech, and the Reconceptualization of Financial Regulation," Northwestern Journal *of International Law and B*usiness 37, no. 3 (2017): 373–415.

Bank for International Settlement. Basel Committee on Banking Supervision Consultative Document Sound Practices for the Management *and Supervision of Operational Risk*, 2017. https://www.bis.org/publ/bcbs183.pdf.

Bank Indonesia, "Laporan Kebijakan Moneter - Triwulan II Tahun 2021," 2021, https://www.bi.go.id/id/publikasi/laporan/Pages/Laporan-Kebijakan-Moneter-Triwulan-II-*2021.aspx*.

Dupuis, Daniel and Kimberly Gleason, "Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic," Journal of Financial Crime, 2020, https://doi.org/10.1108/JFC-06-2020-0113.

Financial Stability Board. "Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention," Financial Stability Board, no. June (2017): 1–61, www.fsb.org/emailalert.

Financial Stability Board. "FSB Report Assesses FinTech Developments and Potential Financial Stability Implications." Www.Fsb.Org, 2019. https://www.fsb.org/wp-content/uploads/P091219-1.pdf.

Frick, T.A (Ed), Financi*al Technology Financial Technology Law* Review (London: Law Business Research Ltd, 2021), 334.

International Compliance Association, "What Is Financial Crime? | ICA," n.d., https://www.int-comp.org/*careers/your-career-in-fi*nancial-crime-prevention/what-is-financial-crime/.

International Monetary Fund, Financial System Abuse, Financ*ial Crime and Mon*ey Laundering, (Washington, D.C: the Monetary and Exchange Affairs and Policy Development and Review Departments IMF, 2001).

Irwin, Angela S.M., Jill Slay, Kim Kwang Raymond Choo, and Lin Lui. "Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study." Journal of Money Laundering Control 17, no. *1 (2014): 50–75. https://d*oi.org/10.1108/JMLC-06-2013-0019.

Irwin, Angela S.M. et al., "Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study," Journal of Mo*ney Laundering Control 17, no. 1 (2014): 50–*75, https://doi.org/10.1108/JMLC-06-2013-0019.

Irwin, Samantha Maitland, Angela, Kim Kwang Raymond Choo, and Lin Liu. "An Analysis of Money Laundering and Terrorism Financing Typologies." Journal of *Money Laundering Control 15, no. 1 (2011): 85–111. htt*ps://doi.org/10.1108/13685201211194745.

Jagtiani, Julapa and Kose John, "FinTech: The Impact on Consumers and Re*gulatory Responses," Journal of Eco*nomics and Business 100, no. November 2018 (2018): 1–6, https://doi.org/10.1016/j.jeconbus.2018.11.002.

Kharisma, Dona Budi, "Mengagas Pembentukan Lembaga Alternat*if Penyelesaian Sengketa (LAPS) Di Sektor Indu*stri Financial Tecnology (FinTech)", Buletin Hukum Kebanksentralan, Vol 17, 2, Juli - Desember (2020), 158-159.

Kharisma, Dona Budi, "Urgency of Financial Technology (FinTech) Laws in Indonesia," Internationa*l Journal of Law and Management 63*, no. 3 (2020): 320–31, https://doi.org/10.1108/IJLMA-08-2020-0233.

Koran Bisnis, "Lima Jaringan Teroris Manfaatkan FinTech, DPR_ Lacak! - Kabar24 Bisnis", 16 April 2021, https://kabar24.bisnis.com/read/20210416*/15/1382110/lima-jaringa*n-teroris-manfaatkan-FinTech-dpr-lacak.

Koran Kompas, "Tersangka Kasus Asabri Cuci Uang Lewat Bitcoin, PPATK_ Modus Baru TPPU Halaman All - Kompas,"22 April 2021, https://nasional.kompas.com/read/2021/04/22/10341781/tersangka-kasus-asabri-cuci-uang-lewat-bitcoin-ppatk-modus-baru-tppu?page=all.

Koran Tempo, "Pandemi Covid-19, OJK_ Investasi Ilegal Marak Bermunculan - Bisnis Tempo," 13 April 2021, https://bisnis.tempo.co/read/1452057/pandemi-covid-19-ojk-investasi-i*legal-marak-bermunculan.*

*Kurum, Esm*an. "RegTech Solutions and AML Compliance: What Future for Financial Crime?" Journal of Financial Crime, 2020. https://doi.org/10.1108/JFC-04-2020-0051.

Lee, David Kuo Chuen and Linda Low, "FinTech in Singapore," Inclusive FinTech, 2018, 307–79, https://doi.org/10.1142/9789813*238640_0008*.

Leong, Kelvin. "FinTech (Financial Technology): What Is It and How to Use Technologies to Create Business Value in FinTech Way?," International Journal of Innovation, Management and Technology 9, no. 2 (2018): 74–78, https://doi.org/10.18178/ijimt.2018.9.2.791.

Merlonghi, Giorgio. "Fighting Financial Crime in the Age of Electronic Money: Opportunities and Limitations," Journal of Money Laundering Control 13, no. 3 (2010): 202–14, https://doi.org/10.1108/13685201011057118.

Muryanto, Yudo Taruno, Dona Budi Kharisma, and Anjar Sri Ciptorukmi Nugraheni, "Prospects and Challenges of Islamic FinTech in Indonesia: *A Legal Viewpoint," Internationa*l Journal of Law and Management, 2021, https://doi.org/10.1108/IJLMA-07-2021-0162.

Naheem, Mohammed Ahmad. "Regulating Virtual Currencies – the Challenges of Applying Fiat Currency Laws to Digital Technology Service*s," Journal of Financial Crime 25, no. 2 (2018): 562–75, https*://doi.org/10.1108/JFC-08-2016-0055.

Ng, Artie W. and Benny K.B. Kwok, "Emergence of FinTech and Cybersecurity in a Global Financial Centre: Strategic Approach by a Regulator," Journal of Financial Regulation and Compliance 25, no. 4 (2017): 422–34, https://doi.org/10.1108/JFRC-01-2017-0013.

Nonaka, Michael. et al., "FinTech in the United States - Regulatory Compliance," Thomson Reuters Practical Law, 2019, 1–17, https://uk.practicallaw.thomsonreuters.com/w-017-4511?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1#co_anchor_a911178.

OJK, "Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Perlindungan Konsumen Pada FinTech," Departemen Perlindungan Konsumen, Otoritas Jasa Keuangan, 2017, hal. 1-86, https://kontak157.ojk.go.id/appkpublicportal/Website/FileShowcase/AttDownload/39.

Pusat Pelaporan Analisis dan Transaksi Keuangan (PPATK), "Perbankan Harus Sigap dan Waspada selama Pandemik Covid-19", 21 August 2021, https://www.ppatk.go.id/siar*an_pers/read/1073/siaran-pers*-kepala-ppatk-perbankan-harus-sigap-dan-waspada-selama-pandemik-covid-19.html.

Rae, Dian Ediana, "Profiling Kejahatan dan Kerentanan Pencucian Uang serta Pendanaan Terorisme sebagai Dampak Krisis Covid-19", Jakarta, 19 August 2021.

Saksonova, Svetlana, and Irina Kuzmina-Merlino, "FinTech as *Financial Innovation - Th*e Possibilities and Problems of Implementation," European Research Studies Journal 20, no. 3 (2017): 961–73, https://doi.org/10.35808/ersj/757.

Santoso, Wimboh "Fi*nTech and The Future of Finance", Surakarta Indonesia, 1*2 March 2020.

Schallmo, Daniel R.A. and Christopher A Williams, Digital Transformation Now! Guiding the Successful Digitalization of Your Business Model D*igitalization of Your Business Mod*el (Switzerland: Springer Nature, 2018).

Sindo News, "Pendanaan Terorisme Kian Canggih, Berubah Seiring Perkembangan Teknologi," 2020, https://nasional.sindonews.com/read/150132/14/pendanaan-terorisme-kian-canggih-berubah-seiring-perkembangan-teknologi-1598893754#:~:text=Tindak%2520pidana%2520pendanaan%2520terorisme%2520(TPPT,currency%2520sebagai%2520sumber%2520kegiatan%2520terorisme.&te.

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," Journal of Financial Crime, 2021, https://doi.org/10.1108/JFC-09-2021-0193.

Teichmann, Fabian M. Johannes. "Financing of Terrorism through the Banking System," Journal of Money Laundering Control 22, no. 2 (2019): 188–94, https://doi.org/10.1108/JMLC-07-2017-0026.

Teichmann, Fabian M. Johannes. "Recent Trends in Money Laundering and Terrorism Financing," Journal of Financial Regulation and Compliance 27, no. 1 (2019): 2–12, https://doi.org/10.1108/JFRC-03-2018-0042.

Teichmann, Fabi*an M. Johannes and Marie Christin* Falker, "Money Laundering via Cryptocurrencies – Potential Solutions from Liechtenstein," Journal of Money Laundering Control, no. January (2020), https://doi.org/10.1108/JMLC-04-2020-0041.

The Chartered Institute for Securities & Investment (CISI), The Background and Nature of Financial Crime (London: CISI, nd).

Treleaven, Philip. "Financial Regulation of FinTech," Journal of Financial Perspectives 3, no. 3 (2015): 114–21.

Wiwoh*o, Jamal and Dona Budi Kharisma, Isu-Isu Hu*kum di Sektor FinTech (Malang: Setara Press, 2021).