Croatian International Relations Review

CIRR

XXVIII (90) 2022, 269-287

DOI 10.2478/ CIRR-2022-0029

UDC 327 (4-6 EU:73:55)

Prevention of Fund Transfer Crime in Modern Banking Practice in Indonesia

Pan Lindawaty Suherman Sewu
Universitas Kristen Maranatha
Email: lindawatysewu@gmail.com
https://orcid.org/0000-0003-0258-7450

Christian Andersen
Universitas Kristen Maranatha
Email: andersen.xtian@gmail.com
https://orcid.org/0000-0002-5974-5803

Hassanain Haykal
Universitas Kristen Maranatha
Email: hassanain.haykal@gmail.com
https://orcid.org/0000-0002-4344-4598

Yohanes Hermanto Sirait
Universitas Kristen Maranatha
Email: yohanessirait1988@gmail.com
https://orcid.org/0000-0001-5678-3188

Rahel Octora
Universitas Kristen Maranatha
Email: octorael@gmail.com
https://orcid.org/0000-0002-6966-2358

Demson Tiopan
Universitas Kristen Maranatha
Email: demson.tiopan@maranatha.edu
https://orcid.org/0000-0003-2446-8591

Shelly Kurniawan
Universitas Kristen Maranatha
Email: shellyelviraa@gmail.com
https://orcid.org/0000-0003-3239-5329

Key words:
Prevention of Fund Transfer, Modern Banking, Indonesia

Abstract

Fund transfer provides some customer convenience, but it can also be exploited as a means of committing crimes that affect people or the state's economy. To identify a new solution, a preventive approach must be implemented. The Police, Central Bank, and Financial Services Authority must collaborate to promote monitoring and systematized funds transfer practice. The government must also enhance regulation and align it with contemporary technologies. This study intends to examine an integrated technique for preventing money transfer crimes. As a normative study, this work investigated data from primary documents (legal material) and secondary documents using qualitative research methods (legal and non-legal material). This article found out that.

Introduction

Since its introduction in the 1960s, information technology has taken over the world by creating interconnected frameworks and technologies that govern persons' daily activities worldwide (Trouet et al., 2018). According to Aspan et al. (2021), between 2015 and 2020, there was an almost 50% growth in internet users and banking penetration in Indonesia.

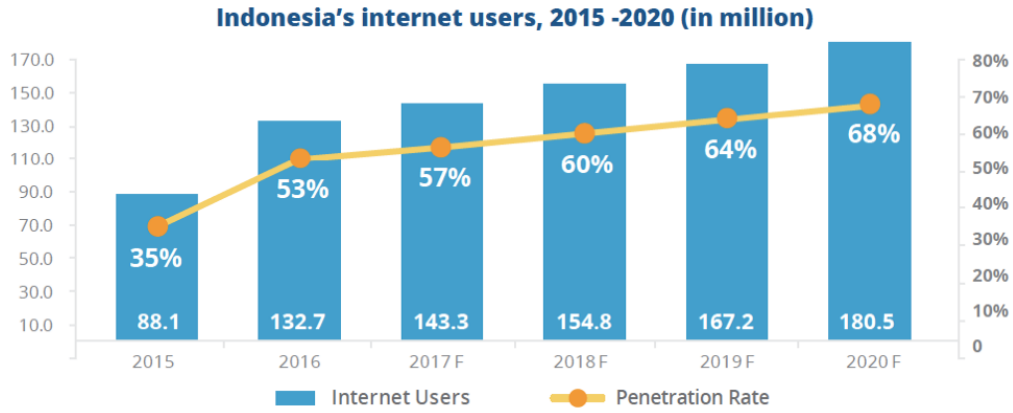

Figure 1. Indonesian Internet Users
Source: (Indonesia, 2017)

The increased accessibility of banking services and the continued trust of clients to maintain vast sums of cash in bank accounts have resulted in the emergence of criminal activities from the modern banking model and the cyber nature of banks. Technological advancements have contributed to the expansion of economies and facilitated the expansion of enterprises and the availability of financial services (F. M. J. Teichmann, 2019). Additionally, technical breakthroughs and economic expansions have contributed to the creation of accessible services such as cash transfers and other digital services, which expose the banking model to criminality and danger. In addition, advances in technology and financial services have contributed to the emergence of new risks and crimes. INCRS reports that the more advanced a country's financial system and economy, the more appealing it is for criminal behavior INCRS, 2017. Money laundering is one

of the most prevalent crimes associated with financial services and banking systems, with a solid association with banking and payment transfers (Putra et al., 2021). The most challenging aspect of combatting money laundering is determining precisely how it occurs. Although numerous global attempts have been made to combat this illicit activity, others say these efforts are insufficient (F. M. Teichmann et al., 2018). According to Karim et al. (2020), technological developments in financial and fund transfer systems contribute to money laundering. Due to the convenience and swiftness of electronic transactions, financial institutions have increasingly relied on electronic money transfers in recent years. For instance, it is possible to complete an electronic transfer in a matter of seconds using ATMs and wire transfers. However, technical advancements that allow legitimate financial transactions also facilitate money laundering. Money laundering thrives with no geographical limitations, 24-hour operations, and swift transactions. Additionally, as information technology progresses and national boundaries become increasingly irrelevant, organized crime prospects are expanding (Faccia et al., 2020; Utami et al., 2020).

Thus, the idea presented in this paper is that modern cash transfers can facilitate criminal activity in banks and other financial institutions. These opportunities expand with the introduction of new technologies. For instance, mobile and online banking have made it easier for fraudsters to exploit security vulnerabilities. Leo Katz states, "The law is full of loopholes." Nobody appears to like them, but they cannot be eliminated for some reason (Johannes Ibrahim et al., 2021). This issue cannot be neglected. To close the loopholes, the government must develop a novel approach. For the law to be effective as a weapon for social change, it must be able to keep up with social change. As previously remarked by Roscou Poung, the law must be capable of serving as an instrument for social engineering. The concept of banking crime is primarily a criminal governed by Indonesia's Banking Law. A crime under this category indicates that it was done solely by a bank or banking company (Reksodiputro, 1994). Banking crime involves funds that the general public has previously deposited in a bank; therefore, this type of crime can harm multiple parties, including both the bank and the customers who deposit their funds, and will spread to the banking system, banking authorities, government, and the larger society. In the practice of the banking industry in Indonesia, the term "banking crime" has not yet been standardized; however, legal experts in Indonesia agree that criminal acts that meet the definition of "banking crime" are those that satisfy the elements outlined in Article 46 to Article 50A of the Banking Law or Article 59 to Article 66 of the Sharia Banking Law.

Regarding the discussion of the results section Illegally Transfer Of Funds As Banking Crimes According to Law No. 3 in the Year 2011, several similar research have been undertaken previously. Benhur Ronal, Riung Olga, A. Pangkerego, and Refly Singal's How to Transfer Funds Online research demonstrates how to classify illegal banking crime according to Law

Number 3 of 2011 and how to resolve Funds Transfer Illegally as a banking crime. However, they do not entirely focus on the prevention concept of fund transfer crimes in Indonesia. Rossa Fadhilah Arista's study, The Role of Bank Indonesia (Bi) In Supervising The System Payment And Protecting Customers Against The Crime Of Skimming (Study On Bank Indonesia Lampung Representative), reveals that the Bank of Indonesia is the supervisor of the system payment in terms of ensuring that the infrastructure is not violated or not violated by criminals (skimmers). Additionally, Fitriya Fauzi, Kenneth Szulczyk, and Abdul Basyith are attempting to commence the prevention and detection of financial crimes (Fauzi et al., 2018). They stress the significance of data sharing in preventing financial crimes such as money laundering. However, the amount of data that can be exchanged is restricted.

These investigations demonstrated that Bank Indonesia requires a service provider's payment system (Bank) to conduct oversight to enhance transaction security and reduce the risk of fraud. In this paper, the researcher focuses on the preventative concept of security in modern technology, data encryption, and the default mode by which the government can appropriately supervise. The laws governing money laundering have not kept pace with the money laundering operations occurring in Indonesian institutions. Thus, research on money laundering in the Indonesian banking industry has the potential to be of great significance. This paper evaluates the legislation governing money laundering, the money laundering operations in Indonesian banks, and the utility of banks as money laundering mobilizers.

The paper takes a descriptive approach in which the first section discusses the status of banking in Indonesia, details the fund transfer operations, and provides a review of the theories that serve as the foundation for this research. The theories of legal gaps and protection were explored, analyzed, and related to case laws. This study explores the research objectives and the primary concerns to be addressed, including the transfer of funds and best practices for preventing the criminal act of transferring cash in Indonesia and other nations. It also examines the prevention of illicit crimes involving the movement of funds in Indonesian banking operations. The final section consists of conclusions and recommendations that provide answers, preventative measures, and methods for resolving difficulties associated with the unlawful conduct of transferring monies.

Literature Review

Concept of Money Laundering

The criminal crime and illegal act of money laundering are described as the concealment of illegal operations that generate enormous sums of money and earnings to "clean" the money (Korejo et al., 2021). Various techniques are used to conceal unlawful activities, such as financial banks, cash businesses, or investments in real estate, stocks, or luxury items, including

gold and diamonds (F. M. J. Teichmann, 2017). While money laundering may appear to be a highly complex and mysterious procedure, it consists of three distinct phases (Faccia et al., 2020). The procedure begins with placement, which is followed by layering and integration. After obtaining the proceeds from illegal activities, the money launderer must deposit the funds into the financial system. He can accomplish this by depositing or transferring funds to banks, national or transnational market businesses, or commercial institutions (Faccia et al., 2020; Wibowo, 2018). By breaking the considerable sum of cash into smaller amounts, the money launderer can make cash deposits into bank accounts or purchase valuable items such as real estate or jewelry (Faccia et al., 2020; F. M. J. Teichmann, 2017). The second phase, called layering, seeks to conceal the initial illicit behavior by executing additional financial transactions (Faccia et al., 2020; Wibowo, 2018). Multiple complex transactions are conducted by layering; for instance, this money will be used to invest in enterprises or purchase shares or real estate. The fragmentation of a substantial amount of cash into smaller amounts makes it challenging to track the original criminal action (Faccia et al., 2020). Integration is the third and last stage of the process. After the preceding step, "clean" money must be poured into the formal economy to make it appear normal and legitimate. Typically, the money is handled through banks so that it appears to be the outcome of corporate activity. Among other methods is the purchase of bonds or securities. The transformation of illicit funds into legal ones that can be utilized for any transaction is complete (Balani, 2019; Faccia et al., 2020). Due to the worldwide nature of money laundering, the scope of this complex crime has extended from drug money to organized crime. There is an urgent need to develop effective anti-money laundering tactics to defend the law and individual rights.

Money laundering phenomenon in Indonesian Banks

Numerous factors place banks at high risk for fraud and money laundering. The expansion of digitalization has facilitated the transportation of funds inside and between nations, but it has also given rise to financial crimes and fraud. In 2010, Indonesia passed the Anti-Money Laundering Law, which established measures to prevent and combat money laundering. Implementation of Regulation No. 12/POJK.01/2017 for Anti-Money Laundering Regulation of the Banking Sector to prevent and halt financing of terrorism in the financial industry (Lukito, 2016). Despite the law's existence, money laundering in Indonesia has alarmed the government. In 2021, the Financial Transaction Reports and Analysis Centre (PPATK) revealed that over 70,000 confusing and suspicious financial transactions were recorded. Approximately 2,4 million suspicious cash transactions were also reported Money laundering is still rife, 2022. In 2016, the General Treasurer of the Democratic Party was sentenced to six years in jail for money laundering. In this case of money laundering, around 500 billion rupees were involved (Sihobing, 2017). Seven banks were victimized by loan applicants and bank employees who collaborated to steal money in a home loan fraud. About 197 fraudulent applications resulted in a loss of

around USD 70 million. The individuals were charged in a case based on anti-money laundering measures (Fauzi et al., 2018). In 2016, the Mayor of Madiun City was accused of transferring funds to other accounts in foreign nations, marking the second instance of money laundering in Indonesia. During his administration, he took bribes and laundered the money with which he was charged by the Indonesian court (Fauzi et al., 2018). Moreover, in 2017, many high-ranking government officials in Indonesia were accused of money laundering and corruption in relation to the electronic resident identity card project (Alamsyah, 2018). In 2017, a former CEO of PT Garuda Indonesia was accused of receiving USD 3 million in bribes, highlighting yet another infamous instance. The bribe money was moved to the ex-mother-in-law CEO and used to purchase assets in Singapore (Fauzi et al., 2018). Multiple prominent and high-ranking figures fell victim to the hoax. In Indonesia, money laundering through financial institutions has become a significant concern. Two bank employees and two others in Badung ostracized the Mandiri Bank robbery. The suspects were charged with violations of the Anti-Money Laundering Act (Alamsyah, 2018).

Funds Transfer and Money Laundering

Initially, concealing criminal actions through the transfer of monies was accomplished using traditional ways, such as passing "dirty" money through informal channels. The usual strategy made it relatively easier for law enforcement to track criminals. Mobile banking, ATMs, and online banking have also evolved as technology has grown. Every region in Indonesia has access to banks, and financial inclusion for low-income groups has expanded through mobile and branchless banking (Kustina, 2017). Cyberpayment systems, which do not require the presence of a third party to transfer money between parties, are defined by the transmission of funds via banks, online or mobile networks (Triyono, 2008). Nevertheless, research suggests that an electronic system for sending cash is problematic owing to interception and fraud (Yeoh, 2020).

With the advent of branchless banking, domestic money transfers are now quite simple. A beneficiary operator or the original operator can transfer funds; nevertheless, the transfer and cancellation processes are governed. International banks are obligated to record and disclose international money transfers. Through its actions, the Indonesian government has classified money transfers as a severe offense. This is evidenced by the fact that Indonesia ratified Law No. 3 of 2011 on Fund Transfer, which is primarily based on Law No. 11 of 2008 on Electronic Information and Transactions and Law No. 8 of 2011 on the Prevention and Eradication of Money Laundering Crimes (Putra et al., 2021). All international transfers in Indonesia are recorded to PPATK through the GRIPS system (APG, 2018). Articles 45 and 53 of the Fund Transfer Regulation govern the provisions for preventing Fund Transfer offenses. Suppose a fund transfer is found to be tied to a criminal act. In that case, many procedures can be taken based on a court's decision or order to annul the transfer of funds

that have already taken place, thereby bolstering efforts to prevent fund transfer crime.

Criminals employ cash transfers as one of their strategies for money laundering. Recently, a new type of money laundering has emerged: a third party employs an individual to accept monies in their bank account. The "money mule" transfers the payments through a bank account or in cash to another individual. The mule may or may not be personally involved in the crime, but he is primarily compensated for his participation. This approach facilitates concealing the flow of transactions (Raza et al., 2020). Fund transfer is the leading contributor to financial crimes in the banking sector. The skimming incident in Bali was a big event that shook the financial banking world. The perpetrators of these atrocities were of various nationalities. Most offenders were Bulgarian, Romanian, and Indonesian (Schmalleger, 2006). Numerous studies have demonstrated that cybercriminals employ internet banking, digital payment mechanisms, and online auctioning for financial crime and money laundering (Chawki, 2022; Mabunda, 2018). The banking industry has established Bank Indonesia Regulation No. 3/10/PBI/2001 about Know-Your-Customer Principles to combat financial crime. Know-Your-Customer Principles are principles banks use to identify as many customers as possible, monitor their trading activities, and report questionable transactions. Applying Know-Your-Customer Principles to face-to-face and non-face-to-face consumers who make telephone calls, correspondence, and internet banking. (Chen, 2020).

Research Methods

This research employs the normative juridical approach, which entails analyzing the literature or secondary data as the primary basis for the analysis. Moreover, this descriptive and analytical study seeks to accurately portray the facts and characteristics of a given topic (Fessha, 2006; Perry, 1995; Ryder, 2011). This study uses the statutory method to examine all statutes and regulations pertinent to the selected legal topic (Fessha, 2006). The data for this study was collected from primary legal sources, such as legislation and regulations pertinent to the topic, and secondary legal sources, including relevant literature studies, articles, and journals. Existing data sources were documented before being evaluated using qualitative, non-numerical methodologies. This study will employ the same methods as prior normative legal studies.

Analysis and Discussion

Problems and Cases in Fund Transfer

The Law on Fund Transfer defines fund transfer as a sequence of acts beginning with the originator who intends to transfer funds to the beneficiary named in the transfer order and concluding with the recipient receiving cash. Crimes involving Fund transfers are considered a white-collar crime due to the culprits' high intelligence and sometimes a well-

established economic background. The use of advanced technologies in the digital and technological realms also characterizes this crime. Several acts that fall under the category of fund transfer crimes in Indonesia have been detailed in Chapter XIII of the Fund Transfer Law's criminal laws, which are as follows:

1. Conducting the activities of Fund Transfer without any permission from Bank Indonesia, including Non-Bank Business Entity;
2. Illegally making or keeping the Fund Transfer Order to use it or order someone else to use it;
3. Using and/or handing over Fund Transfer Order;
4. Illegally taking or transferring part or all of the Funds owned by someone else through False Fund Transfer Order;
5. The beneficiary who knowingly receives or accommodates, either for oneself or others, a Fund which is known or reasonably suspected to come from an illegal Fund Transfer Order;
6. Illegally changing, removing, or deleting part or all of the information contained in the Fund Transfer Order to benefit oneself or others, which results in a loss to the Sender and/or the rightful Beneficiary and/or other parties;
7. Illegally damaging Fund Transfer System;
8. Intentionally controlling and acknowledging as one's property the transfer proceeds known or reasonably known that they are not one's right.

The revelation of the Melinda Dee case stunned the Indonesian banking industry. A top banker from one of the world's largest financial institutions committed a felony by stealing customer monies from CitiBank. This crime cannot be committed by her alone. Acting necessitates assistance from associated work units, such as bank operations and personnel. According to the trial findings, Melinda Dee frequently gives cash and vouchers to hasten her tasks. Since then, Melinda Dee has been charged with violations of the Banking Act and the Money Laundering Act.

In several instances, a man named Didik Agung, posing as a Bank International Indonesia customer, carries out a fraudulent wire transfer on behalf of the fraudster (now called Maybank Indonesia). The instance arose from a technological change to the bank's system; during the process, a system error occurred, resulting in consumers completing transfer transactions without any transfer mutations in their accounts or reductions in their balances. Due to the technological damage, Didik Agung capitalized on the situation. Didik Agung knew that the transfer transaction did not diminish his balance at the time. Didik made multiple transfers on purpose using his and his wife's ATMs since he knew that his balance would not fall. In the end, Didik's acts were uncovered by Maybank, and the bank became aware of Didik's strange transactions. As stated in judgment number 108/Pid.SUS/2014/PN.Skt and Article 3 of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, the judge, found Didik Agung guilty in this case (Lukitasari, 2014).

Moreover, similar to the United States, Articles 2 to 5 of Chapter II of the Law on Fund Transfer govern money laundering offenses involving fund transfer media in Indonesia and reflect on the judgment of the Supreme Court of the Republic of Indonesia No. 1870 K/Pid.Sus/2016 of Defendant Marianda Jumali Abasti a.k.a. Ary J. Absti, it is clear that criminals have modernized their use of fund transfer media to do illegal actions.

Marianda Jumali Abasti alias Ary J. Absti's method of operation consisted of using Moh. Abdul Qader Al Sawae's e-mail to send a confirmation e-mail to Witness Yeni Nuryana (an employee of PT. Yoshin and Moh. Abdul Qader Al Sawae's business partner), stating that "Moh. Abdul Qader Al Sawae paid USD 66 Using an e-mail that appeared to belong to Witness Yeni Nuryana. The offenders then rearranged the order of the wire transfer. Someone is using Moh. Abdul Qader Al Sawae's e-mail address wrote an e-mail to Yeni stating, "Moh. Abdul Al Sawae has made a payment of USD 66,610, but the money has not been received" (the hackers made the e-mail). Due to the inconsistencies in ". ", it was determined that the e-mail was not from Witness Yeni. The contents of the e-mail were identical. Nonetheless, the bank had been changed since the transfer recipient was Bank Central Asia (BCA) with the address of Taman Galaxy Jalan Raya Taman Star, and the account owner is Defendant Marianda Jumali Abasti. The monies were meant to be transferred to PT Bank ANZ Jakarta using account number 41385602000 of PT. Yoshi Utama.

The example of the Supreme Court's ruling cited above is one of the several cases demonstrating how criminals can exploit information technology advancements to help their crimes in the Fund Transfer industry, which in this case are committed by hackers. Therefore, it is vital to strengthen the prevention of Fund Transfer crimes by investigating and analyzing the various preventive efforts of Fund Transfer crimes undertaken by other nations, as well as the feasibility of implementing them in Indonesia and the impediments to their implementation.

Fund Transfer and Best Practices for Fund Transfer Crime Prevention in Indonesia and Several Countries

Fund Transfers, as stated in Article 1 number 1 of Law Number 3 of 2011 concerning Fund Transfers, must be conducted by Fund Transfer operators, as specified in Article 1 number 2, namely Banks and Non-Bank Indonesian Legal Business Entities that execute Fund Transfer activities. In addition, in Article 1 Number 4, the classifications of the Funds transmitted by Fund Transfer operators are elaborated upon as follows:

1. The sender delivers cash to the Beneficiary Operator;
2. Money is deposited in the Sender's Account at the Beneficiary Operator;
3. Money deposited in the Beneficiary Operator's Account at another Beneficiary;
4. Money deposited in the Final Beneficiary Operator's Account;

5. Money deposited in the Beneficiary Operator's account is allocated for the benefit of the beneficiary who does not have an Account at the operator; and/or
6. Overdraft or credit facilities provided by the operator to the sender.

Based on the preceding description, it is evident that banks and non-bank financial firms with legal entities conduct Fund Transfer activities. It turns out, however, that many parties can use this service to their advantage, as seen in Supreme Court Decision No. 1870 K/Pid.Sus/2016 involving Defendant Marianda Jumali Abasti alias Ary J. Absti, who employed technology to control the funds via the Fund Transfer facility. This becomes the Fund Transfer activity's loophole, as Fund Transfer crimes are committed not only in a traditional manner or by individuals who understand the financial system but also in a modern manner by utilizing technology and information media, which any party outside the bank can do.

Observing Law Number 3 of 2011 about Fund Transfer reveals that the emergence of Fund Transfer crimes is linked to the crime of book transfer, which involves transferring a portion or all of another person's cash using a forged draft. Several provisions in the regulations can be used to catch the perpetrators of fund transfer fraud, including Article 81, which states that "the perpetrator must be located first," which could refer to anyone. In this article, it is stated that an individual or an individual who can act as a legal subject can be subject to criminal liability, which means that the perpetrators' actions are prohibited and subject to the law or penal code, particularly the act of taking or transferring particular objects from one location to another voluntarily and knowingly, as well as being fully aware of the consequences of that action, and of obtaining a portion or all of someone else's funds without their consent. This is accomplished through the use of a counterfeit draft, which is a total order from the sender to control the beneficiary to pay a certain amount of money to the beneficiary of the draft, or an activity that begins with the order from the originator to transfer a certain amount of money to the beneficiary named in the draft and continues until the owner receives the unauthorized funds. This article imposes a criminal penalty consisting of imprisonment and fines. In addition to the core criminal punishments, additional criminal sanctions include the requirement to return the proceeds of the crime together with services, interest, or restitution to the victim. In this article, crimes involving the theft or transfer of another person's funds are comparable to fraud or theft with the fund transfer as the purpose. In addition to Article 81, Article 85 may also be enforced if the following conditions are met:

a) In this paragraph, the term "person" refers to any competent human acting as a legal subject with criminal responsibility.
b) Who willfully denotes the individual's desire, knowledge, and awareness of the implications of his action: c) Takes control and recognizes something as his when it is known or should be recognized that it is not his right. Control means that the offender has

authority/power as the possessor of a right to something. In the meantime, acknowledging implies that the offender believes he has the authority/is entitled to something that is his.

In addition, the expanding Fund Transfer crimes frequently view banks as facilitators due to their role as intermediaries in transferring or depositing funds derived from illicit activities. Money Laundering, Crime, and Corruption use Fund Transfer to disguise the beneficial ownership of monies. This is stated in Article 3 of Law Number 3 of 2011 about the Transfer of Funds: "Everyone who places, transmits, switches, expends, pays, donates, entrusts, or takes abroad..." Money Laundering Crime is a follow-up crime in legal studies. In contrast, the principal or initial crime is referred to as a predicate or core offense. If the preceding philosophy is valid, we can define the core crime as the source of the perpetrator's financial gain. In contrast, follow-up crime refers to how the culprit makes the monies earned from his primary crime appear halal or lawful. The culprit commits Fund transfers to launder illicit funds. This has led several nations to classify Fund Transfer crime as serious.

The Financial Action Task Force is a worldwide organization dealing specifically with money laundering concerns (FATF). FATF was the first intergovernmental group to combat money laundering through Fund Transfer crime when it was established in 1989. In 2001, however, the mandate was broadened to cover terrorism financing. FATF coordinates the parts of rules, finances, and law enforcement that are intended to be part of each member nation's national law (Schott, 2006). The United Nations Convention Against Corruption (UNCAC), signed on December 18, 2003, has also been issued. In addition to condemning corruption, the convention addresses efforts to combat the crime of money laundering (addressed explicitly in Article 14). In addition, in Resolution 1617 in 2005, the UN Security Council pushed countries to implement international norms in international anti-money laundering organizations. This recommendation aims to establish international standards for preventing and investigating money laundering crimes (Ahmad Aqeil Mohamad Al-Zaqibh).

In addition, to combat organized crimes such as money laundering and Fund Transfer, the Palermo Convention was established and implemented on September 29, 2003. This convention is the next step after establishing the international organization to combat money laundering. This convention seeks to promote cooperation in preventing and combating organized crime by preserving sovereignty and non-interference in domestic affairs. Among money-laundering prevention policies, policy rules such as customer identification, the adjustment of internal regulations to applicable laws, law enforcement collaboration, and compliance levels require consideration. In the Statement on Preventing Criminal Use of the Banking System for Money Laundering, the Basel Committee mandates this. Since its introduction in 1997, the know-your-customer idea has become one of the most crucial money laundering

prevention principles. There are eleven criteria for evaluating the application of the know-your-customer code.

As a result, the best practices in preventing money laundering in several nations should be investigated further as part of legal renewal initiatives, particularly those addressing the prevention of money laundering related to Fund Transfer offenses. The first rule in the United States to overcome money laundering difficulties was Bank Secrecy Act (BSA), introduced in 1970. The BSA implemented the anti-money laundering program through customer due diligence and screening measures for suspicious transactions. Developed nations also conduct customer due diligence and forensic audits in Singapore to prevent money laundering. In Singapore, for instance, due diligence is required for some deals. A violation of Section 481 of the Corruption, Drug Trafficking, and Other Serious Crimes Act (CDSA) may result in a maximum fine of SGD$ 20,000 for an individual or legal company. The human referred to here is an employee, while the legal entity is an institution or financial organization that violates the law.

Money Laundering, Funds Transfer, And Banking Crimes

Current cybercrimes, such as identity theft, phishing, and smurfing, are prevalent, according to research on financial crimes (Omodunbi et al., 2016; Raza et al., 2020). Surveillance (2019) In the banking sector, the following types of money laundering mechanisms exist in banking practices:

1. Smurfing attempts to escape reporting by dispersing transactions among many culprits.
2. Structuring attempts to circumvent the report by segmenting the transactions to reduce the total number of transactions.
3. U-Turn is an attempt to conceal the origin of criminal proceeds by distorting the transaction and returning the funds to their original account.
4. Cuckoo Smurfing is an attempt to conceal the source of funds by sending the proceeds of crime to the account of a third party who is expecting funds to be sent from abroad and is unaware that the cash he receives is the profits of the crime.
5. The purchase of assets/luxury goods conceals their ownership, including the diversion of assets without detection by the financial system.
5. To evade detection by the financial system, the trade of goods (barter) avoids using monetary funds or financial instruments.
7. Underground Banking/Alternative Remittance Services involve the transfer of funds through an informal, trust-based channel.
8. The use of third parties, in which transactions are conducted using the identity of a third party to prevent the identification of the owner of the proceeds of crime.

To commingle monies is to combine illegally obtained funds with funds from lawful commercial activity to conceal the funds' source. Using false identities implies that the transaction is conducted using a fake identity, making it difficult to trace and detect the identity and existence of money launderers. Using E-Money and Mobile Banking on a vast scale with a bit of nominal is directly related to point g regarding underground banking and ultimately results in money laundering practices. Money launderers conduct instant transactions using virtual credit cards, prepaid sims, and fraudulent bank accounts (Mugarura et al., 2020; Șcheau et al., 2017). Financial thieves can intercept wire transfers into bank accounts, withdraw funds, and make cash withdrawals. In addition, fraudulent documents are utilized to generate reports and corporations through which monies are transferred. The transferred funds are then withdrawn using ATMs (Wronka, 2022). The role of strengthening restrictions through technological detections has been investigated in the banking sector. Using the computer and human profiling tools in banks can aid in the detection of money laundering.

Additionally, banks should strive to make the system traceable and less challenging to enhance the detection of unlawful and fraudulent activity (Colladon et al., 2017; Demetis, 2018). Due to insufficient external and internal supervision, banks become prone to money laundering and fraud, according to researchers. There are almost 17,000 islands in Indonesia, making it challenging to supervise rural banks (Hidajat, 2020). Fraud can be reduced by creating tight bank oversight, complying with regulations and laws, and utilizing big data technologies to detect suspicious activity (Hidajat, 2020).

Comprehensive Attempts to Prevent Fund Transfer Crime in Indonesia

For fund transfer activities, banks and financial institutions must comply with multiple levels of regulation. The regulations may vary between local and foreign banks or between jurisdictions. A bank in Indonesia, for instance, must adhere to Indonesian law, which differs from the rules of another country. Since the topic of this study is Indonesia, Indonesian law applies. Marxen (2019) states that compliance at the domestic level frequently refers to the bank's home jurisdiction. The laws, regulations, and best practice recommendations recognized and enforced in that country apply to any bank or service provider within its borders. Therefore, if a bank operates in multiple countries, it must comply with the rules of each country in which it is operating. Most crimes using electronic information and transactions will involve money transfers in some capacity. Therefore, the legislation about money transfers in Indonesia must be concise and explicit. These regulations should apply to inter- and intra-operator rupiah or foreign currency financial transfers. All sender and recipient operators are headquartered in the Indonesian Republic's Unitary State. Transfers of funds can be made verbally or electronically, and they can occur once or multiple times (Fauzi et al., 2018; Ilmih, 2021;

Karim et al., 2020). Detailed instructions from either the sender or the recipient may authorize a fund transfer. Article 72 of the Financial Transfer Regulation governs the monitoring of fund transfers, and Bank Indonesia carries it out. Bank Indonesia's monitoring process is also carried out with relevant supervisors (Karim et al., 2020). Bank Indonesia can either directly or indirectly monitor banks. Periodically, Bank Indonesia conducts direct inspections, while indirect assessments are accomplished by examining reports and information and conducting fund transfers. Bank Indonesia can also delegate this monitoring to other institutions. Based on the "know your customer" approach, Bank Indonesia Regulation Number 3/10/PBI/2001 governs banking operations in Indonesia meant to detect and eliminate money laundering through fund transfers.

To combat money laundering and terrorism financing more effectively, the Indonesian financial authority has announced new laws. These regulations, including the Financial Services Authority of the Republic of Indonesia Regulation Number 23/POJK.01/2019, replace and supersede the preceding Financial Services Authority Regulation Number 12/POJK.01/2017 about the same subject matter. The IT-based Banking System is being developed increasingly by banking sector participants. The objective is to ensure that clients can enjoy the facilities. In tandem with its development, a system enabling consumers to make real-time payments via an application or financial technology developed collaboratively by start-up enterprises and banking industry participants is created. This is supported by the findings of a poll performed by JakPat and published in Startup Report 2017 DailySocial Id, which indicates that Gopay is the most popular electronic currency and the most popular among the general public. Up to fifty percent of poll respondents had electronic money from Go-Jek, the online transportation service. Meanwhile, e-money from Bank Mandiri and TCASH from Telkomsel, which rated second and third in 2018, has been supplanted; from the bank, only Go Mobile from Bank CU+IMB Niaga placed sixth Databoks, 2021.

PPATK can monitor E-money transactions following its responsibilities and authorities outlined in Law No. 15 of 2002 concerning Money Laundering Crime, as amended by Law No. 25 of 2003. Law Number 8 of 2010 about the Prevention and Eradication of Money Laundering Crime, enacted and proclaimed on October 22, 2010, the PPATK institution was restructured. A cash Transaction Report or CTR is created to prevent the financial services industry from being utilized for money laundering and to detect the placement process. Occasionally, this location can be identified via a Suspicious Transaction Report or STR. Article 13 of the Prevention and Eradication of Money Laundering Regulation governs both reports. Cash transactions of a cumulative value of IDR 500,000,000 (five hundred million rupiahs) or more, in both rupiah and foreign currencies, are required to be reported by law. The primary aspect of tracing financial transactions or the flow of funds is the PPATK's authority in tracing access and authorizing the usage of e-money related to financial and banking operations. It becomes the most straightforward method for ensuring the

commission of crimes, locating their perpetrators, and determining where the proceeds of crime are concealed or camouflaged (Nurmalawaty, 2006). Typically, money launderers in the banking sector have a bank account with a fictitious name, another person's name, or the name of a specific company, which in this case includes account opening by attorneys, accountants, and phony companies. For money laundering, these accounts are used to facilitate the deposit and transfer of unlawful monies, as well as highly sophisticated transaction activities involving several accounts utilizing the identities of numerous individuals, enterprises, or fictitious corporations. Moreover, it is alleged that it is difficult for affiliated banks to determine whether the person who accesses the account is the account's legitimate owner.

Conclusion

One of the crimes that banks are frequently used to facilitate is the fund transfer crime. Fund transfer crime is a sort of fraud, implying it is an act committed by the perpetrator(s) to conduct further crimes. A more specific example would be embezzlement as their primary offense, money laundering as their secondary offense, and fund transfer as an act of the second offense. Indonesia has taken multiple steps to combat money transfer fraud. This article sought to identify the corrective measures made by Indonesia's banking governance and government to remove and regulate money laundering through fund transfers. As technology and information continue to advance, so do criminals' ways of committing fund transfer crimes. A recent instance referenced in the publication was Supreme Court Number 1870 K/Pid.Sus/2016, in which the defendant, Marianda Jumali Abasti alias Ary J. Absti, deceived her victims using information technology media. To address this issue, it is vital to increase the prevention of crimes involving the transfer of funds by enforcing stricter rules and regulations with severe consequences for offenders. Therefore, the review of the literature and actual examples enabled the researcher to make the following suggestions:

1. The government revises the legislation to reinforce it.
2. Educate the public to exercise caution when doing all banking transactions, particularly Fund Transfers.
3. Strengthening cross-sector collaboration (banks, Financial Services Authority and PPATK, Police, and Attorney General's Office) in preventing Fund Transfer crimes and the modernization of the information technology system.

Creating a rule of behavior for bank workers to follow in the event of an emergency in which they uncover the earliest suspicion of a fund transfer crime. Next, research might compare the practices of various states regarding money transfer offenses. It is possible to gain a deeper insight by comparing because cross-border change is significant in the funds' transfer industry.

References

Alamsyah, W. A., Lais; Sunaryanto, A. (2018). Report on the Trend of Corruption Prosecution Cases in 2018. I. C. Watch.

APG. (2018). Anti-money laundering and counter-terrorist financing measures - Indonesia (Third Round Mutual Evaluation Report, Issue. APG.

Aspan, H., & Novita, D. (2021). Legal Arrangements and Issues in E-Commerce. *Tranformative Journal Of Social Sciences, 1*(5), 65-77.

Balani, H. (2019). Assessing the introduction of anti-money laundering regulations on bank stock valuation. *Journal of Money Laundering Control, 22*(1), 76-88. doi: https://doi.org/10.1108/JMLC-03-2018-0021

Chawki, M. (2022). *Cybercrime and the Regulation of Cryptocurrencies.* Paper presented at the Future of Information and Communication Conference: Springer *439*, 694-713. doi: https://doi.org/10.1007/978-3-030-98015-3_48

Chen, T.-H. (2020). Do you know your customer? Bank risk assessment based on machine learning. *Applied Soft Computing, 86*, 105779. doi: https://doi.org/10.1016/j.asoc.2019.105779

Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications, 67*, 49-58. doi: https://doi.org/10.1016/j.eswa.2016.09.029

Demetis, D. S. (2018). Fighting money laundering with technology: A case study of Bank X in the UK. *Decision Support Systems, 105*, 96-107. doi: https://doi.org/10.1016/j.dss.2017.11.005

Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). *Electronic money laundering, the dark side of fintech: An overview of the most recent cases.* Paper presented at the Proceedings of the 2020 12th international conference on information management and engineering, 29-34. doi: https://doi.org/10.1145/3430279.3430284

Fauzi, F., Szulczyk, K., & Basyith, A. (2018). Moving in the right direction to fight financial crime: prevention and detection. *Journal of Financial Crime, 25*(2), 362-368. doi: https://doi.org/10.1108/JFC-06-2017-0060

Fessha, Y. T. (2006). Judicial review and democracy: A normative discourse on the (Novel) Ethiopian approach to constitutional review. *African Journal of International and Comparative Law, 14*(1), 53-82. Retrieved from https://www.euppublishing.com/doi/abs/10.3366/ajicl.2006.14.1.53

Hidajat, T. (2020). Rural banks fraud: a story from Indonesia. *Journal of Financial Crime, 27*(3), 933-943. doi: https://doi.org/10.1108/JFC-01-2020-0010

Ilmih, A. A. (2021). Law Enforcement and Prevention of Banking Criminal Actions in Indonesia. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(3), 5733-5744. doi: https://doi.org/10.17762/turcomat.v12i3.2249

Indonesia, M. R. (2017). Digital Evolution in Indonesia's Banking Industry. Marketresearchindonesia.com; Market Research Indonesia. Retrieved from https://www.marketresearchindonesia.com

Johannes Ibrahim, S., Sirait, Y. H., & SH, L. M. (2021). *Funds Transfer Crime: Evolution and Mode of Crime Through Bank Financial Institution Facilities*: Sinar Grafika (Bumi Aksara). Retrieved from https://books.google.ae/books?hl=en&lr=&id=Z-c_EAAAQBAJ&oi

Karim, A. S., Mohamed, N., Ahmad, M. A. N., & Prabowo, H. Y. (2020). Money Laundering in Indonesia Bankers: Compliance, Practice, and Impact. Retrieved from https://books.google.ae/books?

Korejo, M. S., Rajamanickam, R., & Md. Said, M. H. (2021). The concept of money laundering: a quest for legal definition. *Journal of Money Laundering Control, 24*(4), 725-736. doi: https://doi.org/10.1108/JMLC-05-2020-0045

Kustina, K. T. (2017). MSMEs credit distribution and non-performing loan towards banking companies profit in Indonesia. *Kustina, K., Dewi, I., Prena, G., & Utari, I.(2018). MSMEs Credit Distribution and Non-Performing Loan towards Banking Companies Profit in Indonesia. International Journal Of Social Sciences And Humanities (IJSSH), 2*(1), 10-23. Retrieved from https://ssrn.com/abstract=3683450

Lukitasari, W. N. a. D. (2014). Studi Putusan PN Surakarta Nomor: 108/Pid.SUS/2014/PN.Skt Tindak Pidana Transfer Dana Melalui Perintah Transfer Dana Palsu Yang Dilakukan Oleh Nasabah PT Bank International Indonesia TBK [Study of Surakarta District Court Decision Number: 108/Pid.SUS/2014/PN.Skt Crime of Transferring Funds Through Counterfeit Fund Transfer Orders Made by PT Bank International Indonesia TBK Customers], Recedive. *3*(3), 35.

Lukito, A. S. (2016). Financial intelligent investigations in combating money laundering crime. *Journal of Money Laundering Control, 19*(1), 92-102. doi: https://doi.org/10.1108/JMLC-09-2014-0029

Mabunda, S. (2018). *Cryptocurrency: The new face of cyber money laundering.* Paper presented at the 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD): IEEE, 1-6. doi: https://doi.org/10.1109/ICABCD.2018.8465467

Marxen, K. (2019). International fund transfers in Africa and the compliance measures to detect and combat financial crime-an introduction. *SA Mercantile Law Journal, 31*(2), 261-297. Retrieved from https://hdl.handle.net/10520/EJC-1dfb8dd97c

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control, 24*(1), 10-28. doi: https://doi.org/10.1108/JMLC-11-2019-0092

Nurmalawaty. (2006). Factors Causing the Crime of Money Laundering and Efforts to Prevent it. *Jurnal Equality, 11*, 1-12.

Omodunbi, B., Odiase, P., Olaniyan, O., & Esan, A. (2016). Cybercrimes in Nigeria: analysis, detection and prevention. *FUOYE Journal of Engineering and Technology, 1*(1), 2579-0617. Retrieved from https://core.ac.uk/reader/235186040

Perry, M. J. (1995). Normative indeterminacy and the problem of judicial role. *Harv. JL & Pub. Pol'y, 19*, 375. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals

Putra, I. M. A. M., & Kosasih, J. I. (2021). *Modes of Bank Fund Transfer Crime in Digital Transactions.* Paper presented at the 2nd International Conference on Business Law and Local Wisdom in Tourism (ICBLT 2021): Atlantis Press, 167-171. doi: https://dx.doi.org/10.2991/assehr.k.211203.037

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role of money mules in money laundering and financial crimes a discussion through case studies. *Journal of Financial Crime, 27*(3), 911-931. doi: https://doi.org/10.1108/JFC-02-2020-0028

Reksodiputro, M. (1994). Progress on Economic Development and Crime, (Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum). 74.

Ryder, N. (2011). *Financial crime in the 21st century: law and policy* (Vol. 1): Edward Elgar Publishing. Retrieved from https://books.google.ae/books?hl=en&lr=&id=iRP4el9yPcUC&oi=fnd&pg=PR1&dq=Nicholas+Ryder

Şcheau, M. C., & POP ZAHARIE, S. (2017). Methods of Laundering Money Resulted from Cyber-Crime. *Economic Computation & Economic Cybernetics Studies & Research, 51*(3). Retrieved from ftp://www.ipe.ro/RePEc-old/cys/ecocyb_pdf/ecocyb3_2017p299-314.pdf

Schmalleger, F. (2006). *Criminal law today: An introduction with capstone cases*: Pearson/Prentice Hall Upper Saddle River, NJ. Retrieved from https://www.ojp.gov/ncjrs/virtual-library/abstracts/criminal-law-today-introduction-capstone-cases-third-edition

Schott, P. A. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism* (Vol. 3): World Bank Publications. Retrieved from https://books.google.ae/books?hl=en&lr=&id=qRJlAXxAOCwC&oi=fnd&pg=PR9&dq=Paul

Sihobing, E. (2017). Ex-Democratic Party Treasurer Sentenced to Six Years in Jail in West Sumatra Bribery Case. Retrieved from https://jakartaglobe.id/news/ex-democratic-party-treasurer-sentenced-six-years-jail-west-sumatra-bribery-case/

Surveillance, D. O. F. S. (2019). Guideline on Anti-Money Laundering and Prevention on Terrorism Funding for Banks in Indonesia.

Teichmann, F. M., & Sergi, B. S. (2018). Money Laundering: Challenges and Solutions. In *Compliance in Multinational Corporations* (pp. 31-68): Emerald Publishing Limited, 31-68. doi: https://doi.org/10.1108/978-1-78756-867-920181003.

Teichmann, F. M. J. (2017). Twelve methods of money laundering. *Journal of Money Laundering Control, 20*(2), 130-137. doi: https://doi.org/10.1108/JMLC-05-2016-0018

Teichmann, F. M. J. (2019). Money laundering and terrorism financing through consulting companies. *Journal of Money Laundering Control, 22*(1), 32-37. doi: https://doi.org/10.1108/JMLC-10-2017-0056

Triyono, T. (2008). Analysis of Changes in the Rupiah Exchange Rate Against the US Dollar. *Jurnal Ekonomi Pembangunan, 9*(2), 156 - 167. Retrieved from http://hdl.handle.net/11617/152

Trouet, V., Babst, F., & Meko, M. (2018). Recent enhanced high-summer North Atlantic Jet variability emerges from three-century context. *Nature Communications, 9*(1), 1-9. doi: https://doi.org/10.1038/s41467-017-02699-3

Utami, W., Nugroho, L., Mappanyuki, R., & Yelvionita, V. (2020). Early warning fraud determinants in banking industries. *Asian Economic and Financial Review, 10*(6), 604-627. doi: https://doi.org/10.18488/journal.aefr.2020.106.604.627

Wibowo, M. H. (2018). Corporate Responsibility in Money Laundering Crime (Perspective Criminal Law Policy in Crime of Corruption in Indonesia). *Journal of Indonesian Legal Studies, 3*(2), 213. doi: https://doi.org/10.15294/jils.v3i02.22740

Wronka, C. (2022). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control, 25*(2), 330-344. doi: https://doi.org/10.1108/JMLC-04-2021-0035

Yeoh, P. (2020). Banks' vulnerabilities to money laundering activities. *Journal of Money Laundering Control, 23*(1), 122-135. doi: https://doi.org/10.1108/JMLC-05-2019-0040