



Criminal Liability of Bank Employees in Money Laundering Crimes

Markoni*

Universitas Esa Unggul, Indonesia

Jacky Risman Djuanda
Putra

Universitas Esa Unggul, Indonesia

Imade Kantika

Universitas Esa Unggul, Indonesia

Joko Widarto

Universitas Esa Unggul, Indonesia

***Corresponding author:**

Markoni, Universitas Esa Unggul, Indonesia.

✉ markoni@esaunggul.ac.id

Article Info:

Article history:

Received: July 03, 2026

Revised: July 30, 2026

Accepted: August 06, 2026

Available Online: October 6, 2026

Keywords:

Bank Employees;

Criminal Liability;

Money Laundering Crime;



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2026 by Author. Published by
Politeknik Siber Cerdika International

Abstract

Background: The banking sector plays a strategic role in maintaining national economic stability; however, privileged internal access may expose bank employees to opportunities for committing predicate offenses that lead to money laundering (*Tindak Pidana Pencucian Uang* or TPPU). Insider-facilitated financial crime remains a significant threat to banking systems.

Objective: This study analyzes the construction of criminal liability for bank employees involved in money laundering under Law No. 8 of 2010 and examines the judges' legal considerations in Verdict No. 1002/Pid.Sus/2022/PN Jkt.Tim.

Methods: This normative juridical study employs statutory, case, and conceptual approaches using primary legal materials, including the TPPU Law, Banking Law, Criminal Code (*Kitab Undang-Undang Hukum Pidana* or KUHP), and the relevant court verdict. The materials were analyzed through grammatical, systematic, and teleological legal interpretation.

Results: The findings show that bank employees who divert customer funds through fictitious accounts may bear concurrent criminal liability for the predicate banking offense and subsequent money laundering under a *concursum realis* framework when the statutory elements, including *mens rea* and *actus reus*, are fulfilled. The relevant conduct falls within Articles 3, 4, and 5 of the TPPU Law. The court found that creating fictitious accounts, forging signatures, and transferring IDR 1.2 billion through internal banking applications constituted deliberate acts to conceal the illicit origin of the assets.

Conclusion: The judges' considerations reflect the principles of legal certainty (*Rechtssicherheit*) and utility (*Zweckmäßigkeit*), strengthening the legal framework for addressing insider-facilitated money laundering in Indonesia's banking sector.

To cite this article: Markoni, Putra, J. R. D., Kantika, I., & Widarto, J. (2026). Criminal liability of bank employees in money laundering crimes. *Journal of Law & Social Politics*, 4(4), 1040-1049. <https://doi.org/10.59261/jlsp.v4i4.165>

INTRODUCTION

The banking sector is one of the main pillars in maintaining the stability of Indonesia's national economy (Bhegawati & Utama, 2020; Lesmana & Nuraini, 2025; Widjaja, 2026). Based on its function, banks act as business entities that collect funds from the public in the form of deposits and redistribute them in the form of credit or other financial instruments to improve people's living standards and facilitate payment systems (Challoumis, 2024; Hellman, 1996). Despite playing a vital role, the capital-intensive and digital-based characteristics of the banking industry make it an easy target for various forms of financial crime. One of the most significant threats to the integrity of financial institutions today is banking fraud perpetrated or facilitated by insiders

or employees of the banks themselves.

The United Nations Office on Drugs and Crime (2024) estimated that approximately 2–5% of global GDP is laundered annually, with a significant portion channeled through insider-facilitated schemes within banking institutions. In the Indonesian context, PPATK reported that suspicious financial transaction reports (*Laporan Transaksi Keuangan Mencurigakan* or LTKM) reached 130,472 reports throughout 2023, a 43.78% increase from 2022, with the banking sector accounting for 6.86 million suspicious transactions (PPATK, 2024). The FATF Mutual Evaluation of Indonesia (2023) further highlighted that predicate offenses, including banking fraud, remain classified as high-risk categories for money laundering in the country. These data underscore the urgency of examining the involvement of bank employees in money laundering from the perspective of criminal liability.

The *modus operandi* of white-collar crime within banks' internal environments is evolving rapidly and includes the embezzlement of customer funds, manipulation of authentic data, falsification of credit application documents, and abuse of authority over electronic systems. In its development, banking crime no longer stands alone as a conventional criminal offense but can also constitute a predicate offense for *tindak pidana pencucian uang* (TPPU), or money laundering. Money laundering is an organized and complex mechanism aimed at concealing, disguising, or obscuring the origin of assets obtained through criminal activity so that they appear to be legitimate assets.

The Government of Indonesia has promulgated Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (TPPU Law). This law positions TPPU as an extraordinary crime because of its systemic impact on the economy and public trust. Through this law, legal instruments not only target the principal perpetrators of predicate offenses but also encompass anyone who places, transfers, entrusts, or converts assets that they know or reasonably suspect to have originated from a criminal act.

The involvement of bank employees in money laundering carries a much greater level of risk than that posed by external actors (Esoimeme, 2020; Mat Isa et al., 2025; Tiwari et al., 2020). Bank employees are provided with privileged access to customer databases, authorization over financial transactions, and the intricacies of internal operational systems. This condition makes it easier for them to identify system vulnerabilities and exploit them to conceal the traces of illegal transactions. When employee integrity collapses, the impact can immediately damage the bank's reputation, cause financial losses to customers, and reduce public trust in the stability of the financial system.

This empirical phenomenon of insider crime is concretely reflected in the East Jakarta District Court Decision Number 1002/Pid.Sus/2022/PN Jkt.Tim, in which a bank employee was convicted of illegally using archived customer data to create fictitious accounts and transferring bank funds exceeding IDR 1.2 billion. A detailed analysis of the defendant's *modus operandi* and the fulfillment of the elements of the criminal offenses is presented in the Results and Discussion section.

Academically and practically, juridical problems arise regarding how to construct criminal liability for bank employees who bear dual criminal liability for both the predicate banking offense and the subsequent money laundering offense. Is it sufficient for law enforcement to stop at the conventional provisions governing embezzlement, or should the conduct also be addressed under the TPPU legal regime in order to optimize asset recovery? Based on the above background, this article examines in depth the criminal liability of bank employees in TPPU cases and analyzes the *ratio decidendi* considered by the judges in rendering a judgment in Case Number 1002/Pid.Sus/2022/PN Jkt.Tim.

Previous studies have examined money laundering from regulatory and institutional perspectives. Simanjuntak & Jha (2025) analyzed AML frameworks in Indonesian banking, while Kurum (2023) explored RegTech solutions for AML compliance. However, these studies focused predominantly on institutional compliance mechanisms rather than the individual criminal liability of bank employees who act as self-launderers of the proceeds of predicate offenses. The present study fills this gap by constructing a criminal liability framework specifically for bank employees who commit predicate offenses and subsequently launder the proceeds, analyzed

through the lens of an actual court decision. This constitutes the novelty of this research: integrating doctrinal criminal liability theory with a case-based analysis of insider-facilitated self-laundering in the Indonesian banking sector.

METHOD

This legal research used a normative legal research methodology. The main focus of normative legal research was to examine positive legal norms, legal principles, legal doctrines, and the vertical and horizontal synchronization of applicable laws and regulations related to the legal issues under study. The legal approaches applied to explore the problems in this study comprised three types of approaches: the statute approach, the case approach, and the conceptual approach. The statute approach was used to examine the consistency of the provisions contained in Law Number 8 of 2010 concerning TPPU and Law Number 10 of 1998 concerning Banking. The case approach was carried out by studying, interpreting, and analyzing the judges' legal considerations (*ratio decidendi*) and judgment in Criminal Case Number 1002/Pid.Sus/2022/PN Jkt.Tim. The conceptual approach referred to doctrines of criminal law, theories of criminal liability, and concepts of banking law put forward by leading scholars to construct sound legal arguments.

The data sources used in this study relied entirely on secondary data, which were grouped into three categories of legal materials: primary, secondary, and tertiary legal materials. Primary legal materials consisted of banking laws, the TPPU Law, the ITE Law, the Criminal Code (KUHP), and the official copy of the East Jakarta District Court Decision Number 1002/Pid.Sus/2022/PN Jkt.Tim. Secondary legal materials consisted of criminal law textbooks, national and international scientific journals, symposium proceedings, and legal opinions of experts. Tertiary legal materials consisted of legal dictionaries, encyclopedias, and information obtained from relevant Internet sources.

The data collection method was carried out through library research using in-depth inventory, classification, and document-recording techniques, supplemented by online research. All collected legal materials were then analyzed using normative qualitative analysis. The analysis focused on grammatical, systematic, and teleological legal interpretation, as well as legal reasoning, to answer the research questions comprehensively. The legal interpretation methods employed in this study comprised: (1) grammatical interpretation, which was used to analyze the textual meaning of statutory provisions in the TPPU Law and Banking Law; (2) systematic interpretation, which was applied to examine the coherence and interrelationship of legal norms across different statutes; (3) teleological interpretation, which was utilized to identify the legislative purpose and policy objectives underlying the TPPU Law; and (4) comparative interpretation, which was employed to situate the Indonesian legal framework within the broader international AML legal discourse (Ibrahim, 2012). These methods were applied in conjunction with deductive legal reasoning to construct comprehensive answers to the research questions.

RESULTS AND DISCUSSION

Results

Construction of Criminal Liability of Bank Employees in the Anti-Money Laundering (TPPU) Law Regime

In criminal law discourse, criminal liability or responsibility is a fundamental instrument for determining whether an individual may be subjected to criminal sanctions for unlawful acts or events. This concept concerns not only legal considerations but also moral values or the general morality embraced by a society or groups within society. This is intended to ensure that criminal accountability is achieved in accordance with the principle of justice. In Indonesia, criminal liability is firmly based on the legal principle of "no crime without fault" (*nulla poena sine culpa* or *geen straf zonder schuld*). This means that criminal liability may arise only when a criminal act has been committed and the elements of the offense prescribed by law have been fulfilled. The application of criminal liability requires an assessment of whether the facts of an event correspond to the statutory elements of the relevant criminal offense. In other words, the existence of an unlawful act (*actus reus*) must be accompanied by fault in the form of intent (*dolus*)

or negligence (*culpa*) on the part of the perpetrator (*mens rea*).

According to Roeslan (1983), a person may be held criminally responsible only if that person has committed an act with fault. For an offense to result in a person's conviction, four basic cumulative elements must be satisfied, namely: (1) the commission of a criminal act; (2) the capacity to be held responsible; (3) the commission of the act intentionally or through negligence (*culpa*); and (4) the absence of grounds for excuse. When these elements are applied to bank employees as legal subjects, their position becomes particularly important. Based on the doctrine of banking law, the definition of bank employees is not limited to front-office staff who have direct contact with customers but also includes employees involved in daily banking activities, such as operations, credit, treasury, compliance, and internal audit, who perform their duties within the scope of their respective functions and authorities. In the context of banking criminal law, bank employees occupy an important position because they are among the first parties to have access to customer data and transactions. Consequently, they may also have the opportunity to abuse their authority to commit criminal acts, including money laundering, making a strict system of internal supervision and controls necessary.

Money laundering crimes (*TPPU*) involving internal bank personnel are generally associated with insider crime, which can be particularly dangerous because the perpetrator understands the vulnerabilities and weaknesses of the system from within. Sjahdeini (2007) stated that money laundering is a dual-offense phenomenon because it always begins with an underlying or predicate crime and is subsequently followed by acts intended to conceal or disguise the proceeds of that crime. The principal characteristic of money laundering is that it does not stand independently in an economic sense but is preceded by an underlying criminal offense that generates illicit proceeds. According to Sjahdeini (2007), banking fraud encompasses forms of unlawful conduct committed in banking activities by both internal and external parties that may harm customers and undermine the stability of the financial system. Within the banking sector, the underlying or predicate crime may manifest itself through banking fraud, such as the misuse of access to customer data and banking systems, manipulation of financial transaction mechanisms, abuse of authority to transfer funds, fictitious account opening, and manipulation of bank records.

The legal framework governing the prosecution of bank employees who commit money laundering is primarily regulated in Chapter II of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes. Any person who carries out acts involving assets that he or she knows or reasonably suspects to be the proceeds of a criminal act may be subject to criminal sanctions. The typology of the perpetrator's conduct may be categorized into three principal offense clusters:

1. Active Perpetrator (Article 3 of Law No. 8/2010): Every person who places, transfers, pays, grants, donates, entrusts, brings abroad, changes the form of, exchanges for currency or securities, or performs other acts involving assets that he or she knows or reasonably suspects to be the proceeds of a criminal act, with the purpose of concealing or disguising the origin of such assets.
2. Concealment or Disguising Offense (Article 4 of Law No. 8/2010): Any person who conceals or disguises the origin, source, location, designation, transfer of rights, or actual ownership of assets that he or she knows or reasonably suspects to be the proceeds of a criminal act.
3. Passive Offender (Article 5 of Law No. 8/2010): Any person who receives or controls the placement, transfer, payment, grant, donation, custody, exchange, or use of assets that he or she knows or reasonably suspects to be the proceeds of a criminal act.

The current legal framework primarily addresses individual criminal liability, whereas the concept of corporate criminal liability for banking institutions that fail to implement adequate internal controls remains underdeveloped in Indonesian law. Internationally, the landmark TD Bank case in 2024, in which the institution pleaded guilty to conspiracy to commit money laundering and was fined approximately USD 3.09 billion, demonstrates the growing trend toward holding financial institutions corporately liable for systemic AML failures (U.S. Department of Justice, 2024). Future studies in the Indonesian context should examine whether

banking institutions can be held criminally liable for systemic failures in their AML compliance programs that facilitate insider-driven money laundering (Lokanan, 2023; Ofoeda et al., 2024).

Comparative Theoretical Analysis: The Limitations of Grounds for Excuse in Cases of Negligence by Banking Personnel

When the doctrinal views are examined comparatively, there is both a common thread and a clear distinction between the thoughts of Roeslan (1983) and Hamzah (1994) concerning the existence of grounds for excuse (*schulduitsluitingsgronden*) when applied to negligence by banking personnel. Roeslan Saleh emphasized that one of the principal elements of fault is the absence of grounds for excusing the perpetrator, while the capacity to be held responsible must be assessed from both psychological and normative perspectives. In the realm of banking professionals, Roeslan Saleh's theoretical view suggests that deviations from operational standards committed by an employee cannot automatically be shielded by characterizing the conduct as "ordinary administrative negligence" if the act consciously creates or exploits a substantial opportunity for actual loss. A person possessing specialized skills, occupying a managerial position, or exercising authority over financial operations is expected to have sufficient mental capacity to anticipate the risks associated with his or her conduct. Accordingly, the scope for an excuse becomes considerably narrower when the individual consciously disregards fundamental compliance obligations.

On the other hand, Hamzah (1994) provides a complementary explanation that criminal liability constitutes a person's responsibility for bearing the criminal consequences of unlawful conduct when the element of fault is established. Regarding the limitation of grounds for excuse in cases of negligence in the performance of official duties, Andi Hamzah's thinking distinguishes serious negligence (*culpa lata*) from minor negligence (*culpa levis*) and from purely administrative errors. If the negligence of a bank employee occurs because of unavoidable psychological coercion (*overmacht*) or because of systemic instructions from bank leadership that formally appear legitimate but are in fact manipulative or unlawful, the availability of a ground for excuse may be examined in light of the specific circumstances of the case. However, if the negligence constitutes gross negligence that violates the prudential principles applicable to banking, there may be no legal basis for an excuse capable of eliminating criminal fault. This is because the employee's failure to comply with professional competency and prudential standards may constitute the basis for attributing fault to the employee in light of the responsibilities inherent in his or her position.

Typology of Money Laundering in Electronic Banking Transactions

According to Adrian Sutedi (2018), money laundering generally constitutes a method of concealing, transferring, and using the proceeds of criminal acts, including the activities of criminal organizations, economic crimes, corruption, narcotics trafficking, and other criminal activities. Money laundering essentially involves assets or proceeds that are disguised so that they can be used without detection of their illicit origin. Through money laundering activities, income or wealth derived from unlawful activities is converted or transformed into financial assets that appear to originate from legitimate sources or lawful transactions. Based on Sutedi (2008) theory, this cycle of illicit fund movement operates through three distinct stages that can be identified within the electronic banking transaction ecosystem:

1. Placement: This is the earliest stage in the money laundering cycle, in which the perpetrator attempts to introduce proceeds of crime, particularly cash, into the formal financial system. In the context of modern electronic banking transactions, the placement process is no longer limited to physically depositing cash at a teller counter. It may also involve the abuse of internal authorization to create or manipulate digital account balances, the manipulation of customer deposit data, cash deposits through ATM networks, or the use of fictitious accounts. This stage aims to transform or introduce the proceeds of crime into forms that can be transferred or otherwise circulated through the financial system without immediately triggering suspicion.
2. Layering: After the funds have entered the banking system, the perpetrator proceeds

to the layering stage by conducting a series of complex, successive, and often rapid financial transactions designed to distance the assets from their original criminal source or predicate crime. In electronic banking, this stage may involve electronic funds transfers, cross-jurisdictional transfers through clearing networks or the Real-Time Gross Settlement (RTGS) system, foreign-currency conversion, and *smurfing*, in which transactions are divided into smaller amounts. The use of mobile banking and internet banking applications may facilitate the obscuring of the digital audit trail, thereby making it more difficult for financial intelligence and law-enforcement authorities to trace the original source of the funds.

3. Integration: This is the final stage, in which wealth that has been layered and its illicit origins obscured is reintroduced into legitimate economic activity so that it appears to constitute lawful and legitimate assets. In the electronic banking environment, integration may occur when funds held in accounts used during the layering process are withdrawn electronically, invested in digital mutual funds or other investment portfolios, used to purchase valuable assets such as property or financial instruments through electronic-commerce platforms, or used to finance legitimate business activities. At this stage, illicit funds have become sufficiently commingled with legitimate financial activity that the perpetrator may use or enjoy the proceeds while attempting to conceal their connection to the original criminal act.

Case Analysis: Decision Number 1002/Pid.Sus/2022/PN Jkt.Team and the Judges' Legal Considerations

The factual circumstances described in East Jakarta District Court Decision Number 1002/Pid.Sus/2022/PN Jkt.Team provide a concrete illustration of how a money laundering *modus operandi* may be carried out from within a financial institution. This case involves a defendant named Novaldi Pratomo, a bank employee who possessed operational authority over the bank's internal documentation and data.

Anatomy of the Defendant's Modus Operandi*

The *modus operandi* employed by the defendant may be classified into three stages of structured financial crime:

1. First Stage (Misuse of Data and Documents): The defendant dismantled and accessed old files relating to previous customer credit applications stored in the bank's system. The customers' authentic personal data was taken and reused without authorization to facilitate the opening of new fictitious accounts.
2. Second Stage (Fraud and Forgery): To activate and pass the verification process for the fictitious accounts, the defendant forged customers' signatures on account-opening applications and card specimen sheets. The defendant then used his electronic access privileges to enter the bank's internal application and manipulate the authorization process for transferring the bank's operational funds to the fictitious accounts. The total amount of funds successfully misappropriated reached IDR 1.2 billion.
3. Third Stage (Money Laundering—Layering and Integration): Once the funds had been transferred to a fictitious account used as a holding account, the defendant gradually transferred the funds to his personal account as well as to other third-party accounts. This step was intended to complicate the tracing of the funds through the bank's internal compliance and audit systems. The funds were eventually withdrawn in cash and used for the defendant's personal interests and consumption.

The foregoing conduct demonstrates the combination of predicate offenses, including forgery, fraud, embezzlement or misappropriation in the performance of office, and potentially offenses involving electronic systems, followed by the money laundering offense referred to in Article 3 of Law Number 8 of 2010.

Article-by-Article Juridical Review Based on the ITE Law of the Defendant's Actions

If the defendant Novaldi Pratomo's alleged manipulation of authentic bank data is

analyzed under the legal framework of the Law on Electronic Information and Transactions (ITE Law), the conduct must be assessed carefully against the specific elements of Articles 30, 31, and 32. The article-by-article juridical review is as follows:

1. Analysis of Article 30 of the ITE Law (Illegal Access): This article prohibits any person from intentionally and without authorization or unlawfully accessing a Computer and/or Electronic System belonging to another person in any manner. The legal facts indicate that, although Novaldi Pratomo was a bank employee with authorized access for official purposes, he allegedly acted "without rights and against the law" when he used his electronic credentials to access archived customer credit applications and enter the internal authorization system beyond the scope of his functional authority. The use of authorized credentials for an unauthorized criminal purpose does not, by itself, automatically establish every element of Article 30; rather, the prosecution must establish that the access was without authorization or otherwise unlawful within the meaning of the statute. If established, such conduct may satisfy the elements of unauthorized access under Article 30 of the ITE Law.
2. Analysis of Article 31 of the ITE Law (Illegal Interception): This article regulates the prohibition against intentionally and without authorization or unlawfully intercepting or tapping Electronic Information and/or Electronic Documents in or from a Computer and/or Electronic System. The mere collection, copying, or recording of personal data from electronic documents does not necessarily constitute "interception" within the meaning of Article 31. Accordingly, the application of Article 31 requires proof that the defendant intercepted or tapped an electronic transmission as contemplated by the statutory provision. If the defendant merely accessed, copied, or extracted information from stored electronic documents, the conduct may instead be more appropriately analyzed under the provisions governing unauthorized access or unlawful manipulation or transfer of Electronic Information and/or Electronic Documents.
3. Analysis of Article 32 of the ITE Law (Data Manipulation or Unlawful Transfer): This article prohibits any person who intentionally and without authorization or unlawfully, in any manner, alters, adds to, reduces, transmits, damages, deletes, moves, conceals, or otherwise transfers Electronic Information and/or Electronic Documents belonging to another person or to the public. Novaldi Pratomo's alleged manipulation of the bank's internal applications and electronic records may therefore be analyzed under Article 32, provided that the prosecution establishes that the relevant conduct concerned Electronic Information and/or Electronic Documents and satisfied the other statutory elements. In particular, the alteration, movement, or unlawful transmission of electronic banking records or data may fall within the scope of Article 32. However, the transfer of IDR 1.2 billion itself should not automatically be characterized as an Article 32 offense merely because it was executed electronically; the legal analysis must identify the specific electronic information or electronic document that was altered, transmitted, moved, or otherwise manipulated.

Analysis of the Judges' Ratio Decidendi

In imposing a guilty verdict against the defendant Novaldi Pratomo, the panel of judges of the East Jakarta District Court applied a comprehensive method of legal consideration (*ratio decidendi*), encompassing the aspects of legal certainty (*rechtssicherheit*), justice (*gerechtigkeit*), and utility (*zweckmäßigkeit*).

According to Mertokusumo (1988), a judicial decision is a statement made by a judge, as a state official authorized to issue such a decision, pronounced in court for the purpose of ending or resolving a case or dispute between the parties. It is not only the statement delivered orally that constitutes a judicial decision, but also the statement set out in written form and subsequently pronounced by the judge at trial. A written decision does not have the force of a judicial decision before it has been pronounced at trial by the judge. From the perspective of substantive legal considerations and the formal application of evidentiary rules, the panel of

judges described the fulfillment of the elements of Article 3 of Law Number 8 of 2010 as follows:

1. The Element of "Every Person": Referring to the individual legal subject, namely the defendant Novaldi Pratomo, who was shown to be mentally and physically capable of participating in the proceedings and answering questions at trial, he was categorized as a legal subject capable of being held criminally responsible in accordance with the theory of criminal responsibility.
2. The Elements of "Placing, Transferring, and Otherwise Dealing with Assets": The trial facts established that the defendant transferred funds amounting to IDR 1.2 billion from the bank's operational funds to a fictitious account and subsequently forwarded the funds to his personal account using an internal banking application. This conduct was considered to satisfy the substantive element concerning the transfer or other dealing with assets as prohibited by Article 3.
3. The Element of "What He Knew or Should Have Suspected Was the Proceeds of a Criminal Act": The judges found this element to be satisfied because the defendant was fully aware that the IDR 1.2 billion did not belong to him and had been obtained through unlawful means, including the forgery of documents and customer signatures. Accordingly, the court found a direct connection between the predicate crime and the assets that were subsequently subjected to money laundering.
4. The Element of "With the Purpose of Concealing or Disguising the Origin of the Assets": The pattern of transferring funds from the bank's operational funds to fictitious accounts held in another person's name before ultimately transferring the funds to the defendant's personal account was considered by the judges to constitute an intentional effort to conceal or disguise the origin and movement of the funds and to impede the tracing of their actual ownership and control, including the identification of the relevant beneficial owner.
5. The judges also included sociological considerations and economic impacts in their decision. Crimes committed by insiders present a significant level of social danger because they undermine the principle of trust that constitutes a fundamental foundation of the banking industry. The defendant's conduct was considered to have undermined the integrity and professional obligations of the banking profession, including the obligation to implement good corporate governance.

Therefore, the imposition of a prison sentence combined with a substantial fine in this decision was considered proportionate. The judges' decision in this case is normatively assessed as reinforcing the commitment to strict law enforcement against insider-facilitated money laundering while upholding legal certainty that the abuse of professional authority by bank employees will be addressed through appropriate and layered legal instruments designed to protect the economic stability and interests of the wider community.

CONCLUSION

The construction of criminal liability for bank employees involved in the Crime of Money Laundering (*Tindak Pidana Pencucian Uang* or TPPU) is based on the cumulative fulfillment of the elements of guilt (*mens rea*) and unlawful conduct (*actus reus*). Under Law Number 8 of 2010, bank employees may be categorized as active perpetrators under Article 3 if they are proven to have used their position and access rights to transfer assets that they know or have reasonable grounds to suspect are derived from the proceeds of criminal activity. Given their professional expertise and their obligation to observe the prudential principle, the element of reasonable suspicion regarding the unlawful origin of a transaction is particularly relevant to bank employees. Their criminal liability is independent and may be multi-layered, with the underlying criminal offense prosecuted alongside money laundering charges to optimize the recovery of state assets and assets belonging to banking institutions.

The judge's legal considerations in Decision Number 1002/Pid.Sus/2022/PN Jkt.Team are assessed as consistent with the normative principles of legal certainty, justice, and utility in addressing insider-facilitated money laundering. The judge carefully established that the defendant's actions, including creating fictitious accounts, forging signatures, and transferring

Rp1.2 billion through internal banking applications to personal accounts, constituted concrete acts intended to conceal and disguise the origin of illicit assets. The judge's decision to impose severe criminal sanctions was based, among other considerations, on the sociological impact of white-collar crimes committed by banking insiders (insider crime), which can undermine public trust in the banking system, compromise banking integrity, and adversely affect national macroeconomic stability. This decision upholds the principles of justice and legal utility and may serve as a normative precedent for stricter enforcement against insider-facilitated money laundering within the Indonesian financial industry.

Based on these findings, the authors recommend that banking institutions strengthen their internal control systems through technology-based supervision mechanisms, including real-time transaction monitoring, anomaly-detection algorithms, and enhanced Know Your Customer (KYC) procedures integrated with the PPATK's goAML reporting system. Furthermore, periodic compliance audits, whistleblower protection programs, and mandatory anti-money laundering (AML) training for all bank employees should be institutionalized to prevent and detect insider-facilitated financial crimes at the earliest possible stage.

ACKNOWLEDGEMENT

The authors express their appreciation to all parties who provided academic support and constructive feedback during the preparation of this research. The authors also acknowledge the editors and reviewers whose comments contributed to improving the clarity and quality of the manuscript.

AUTHOR CONTRIBUTION STATEMENT

Markoni, Jacky Risman Djuanda Putra, Imade Kantika, and Joko Widarto jointly contributed to the conceptualization of the study, collection and review of legal materials, legal analysis, interpretation of the findings, and preparation of the manuscript. All authors reviewed, contributed to, and approved the final version of the manuscript and accept responsibility for its content.

REFERENCES

- Adrian Sutedi, S. H. (2018). *Tindak pidana pencucian uang*. PT Citra Aditya Bakti.
- Bhagawati, D. A. S., & Utama, M. S. (2020). the Role of Banking in Indonesia in Increasing Economic Growth and Community Welfare. *South East Asia Journal of Contemporary Business, Economics and Law*, 22(1).
- Challoumis, C. (2024). Demystifying the banking system: The importance of the money cycle. *SSRN Electronic Journal*.
- Esoimeme, E. E. (2020). Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules. *Journal of Money Laundering Control*, 24(1). <https://doi.org/10.1108/JMLC-05-2020-0053>
- Financial Action Task Force (FATF). (2023). Mutual Evaluation Report: Anti-Money Laundering and Counter-Terrorist Financing Measures – Indonesia. FATF.
- Hamzah, A. (1994). *Asas-asas hukum pidana*.
- Hellman, T. (1996). Development finance as institution building: A new approach to poverty-oriented banking. *Journal of Development Economics*, 50(2). [https://doi.org/10.1016/s0304-3878\(96\)00411-7](https://doi.org/10.1016/s0304-3878(96)00411-7)
- Kurum, E. (2023). RegTech solutions and AML compliance: what future for financial crime? *Journal of Financial Crime*, 30(3). <https://doi.org/10.1108/JFC-04-2020-0051>
- Lesmana, A. Y., & Nuraini, A. (2025). Factors Affecting the Stability of Financial Banking System in Indonesia. *Nominal: Barometer Riset Akuntansi Dan Manajemen*, 14(2).
- Lokanan, M. E. (2023). Financial fraud detection: the use of visualization techniques in credit card fraud and money laundering domains. *Journal of Money Laundering Control*, 26(3), 436–444. <https://doi.org/10.1108/JMLC-04-2022-0058>
- Mat Isa, Y., Mohd Sanusi, Z., Prabowo, H. Y., & Tarjo, T. (2025). Routine activity theory and the dynamics of money laundering: reassessing emerging threats in banking operations.

- Journal of Money Laundering Control*. <https://doi.org/10.1108/JMLC-06-2025-0106>
- Mertokusumo, S. (1988). Hukum Acara Perdata Indonesia Edisi Ketiga. *Liberty, Yogyakarta*.
- Ofoeda, I., Agbloyor, E., & Abor, J. Y. (2024). Financial sector development, anti-money laundering regulations and economic growth. *International Journal of Emerging Markets*, 19(1), 191–210. <https://doi.org/10.1108/IJOEM-12-2021-1823>
- PPATK. (2024). Laporan Tahunan 2024: Pusat Pelaporan dan Analisis Transaksi Keuangan. Jakarta: PPATK.
- Roeslan, S. (1983). *Perbuatan Pidana dan Pertanggungjawaban Pidana.* Dua Pengertian Dasar dalam Hukum Pidana. Jakarta: PT. Aksara Baru.
- Simanjuntak, E. L., & Jha, G. K. (2025). Strengthening the Gatekeeper Function of Banks: The Role of KYC in Anti-Money Laundering Legal Framework. *Lex Publica*, 12(2). <https://doi.org/10.58829/lp.12.2.2025.320>
- Sjahdeini, S. R. (2007). *Seluk beluk tindak pidana pencucian uang dan pembiayaan terorisme*.
- Sutedi, A. (2008). *Hukum Perbankan: Suatu Tinjauan Pencucian Uang, Merger, dan Kepailitan*. Bandung: Citra Aditya Bakti.
- Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. In *Pacific Accounting Review* (Vol. 32, Number 2). <https://doi.org/10.1108/PAR-06-2019-0065>
- United Nations Office on Drugs and Crime (UNODC). (2024). Money Laundering Overview. UNODC.
- U.S. Department of Justice. (2024). TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations [Press Release].
- Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.*
- Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.*
- Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.*
- Widjaja, G. (2026). Banking regulations as instruments for regulating national economic activities: A comprehensive literature review of the role of Bank Indonesia and the Financial Services Authority in achieving financial stability, sustainable economic growth, and modern payment system integration. *International Journal of Financial Economics*, 2(7), 1354–1364.