JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 2 Mei 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i2.10612/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Bank's Legal Responsibility in Detecting *Shadow Controller-Related Beneficial Owner*

Wawan Zulmawan[1], Daniel Johnson Goenawan[2], Marchello Putra Toding Palilli[3], Ramdhan Mahardika Nasyith[4], Muhamad Naufal Rionatadiraja[5], Reyzel Yandika Lim[6], Triswer[7]

Article Info

Article history:
Received: 30 April 2026
Publish: 9 May 2026

Keywords:
Tanggung Jawab Bank;
Shadow Controller;
Beneficial;
Owner.

Abstract

Transparency of legal entity ownership through reporting Beneficial Owner (BO) to the Ministry of Law and Human Rights is an important policy in preventing Money Laundering. However, the practice of shadow controllers, parties who de facto control a legal entity but are not reported as BO, remains a serious loophole. Banks as gatekeepers of the financial system have a strategic position to detect shadow controllers. This article aims to analyze the legal liability of banks for failing to detect shadow controllers, the sanctions that may be imposed, and the standard of proof for constructive knowledge. This research uses normative legal method with statutory and conceptual approaches, examining the Banking Law (Law No. 7/1992 as amended by Law No. 4/2023 on P2SK), Anti-Money Laundering Law No. 8/2010, OJK Regulation No. 8/2023 on APU-PPT, and Ministry of Law Regulations No. 2/2025 and No. 49/2025 on corporate BO. The results show that bank liability is fault-based, not strict liability. Banks that ignore indications of shadow controllers may be subject to administrative sanctions (reprimands to license revocation), civil sanctions (damages claims), and criminal sanctions. The standard of proof for constructive knowledge uses objective indicators such as suspicious transactions, complex ownership structures, and discrepancies between official documents and customer operational reality, measured by the reasonableness principle (prudent banker). This article recommends that banks act proactively by conducting independent verification beyond merely relying on the Ministry's BO reports, and strengthen early detection systems against shadow controllers.

Corresponding Author:
Wawan Zulmawan
Universitas Pelita Harapan
Email: wawanzul2003@gmail.com

1. INTRODUCTION

In recent years, the issue of transparency in legal entity ownership has become a significant concern in Indonesia's legal and financial systems. This is due to the increasing complexity of economic activity and the widespread misuse of legal entities as a means to conceal the identity of their true owners. To address this challenge, the Indonesian government, through the Ministry of Law and Human Rights (Kemenkumham), requires all legal entities, such as Limited Liability Companies (PT), foundations, cooperatives, and other entities, to report their beneficial owners (BO). This policy aims to ensure that the state has clear data on who truly controls and benefits from a legal entity, not just those administratively registered in official documents.

Beneficial Owner refers to an individual who directly or indirectly can control a legal entity, either through share ownership, voting rights, or significant influence in decision-making. In practice, a person can be categorized as a Beneficial Owner even if their name is not listed as a majority shareholder, as long as they have actual control over the company (Pradhana et al., 2025). Therefore, Beneficial Owner reporting is an important tool for breaking through the layers of formality that often obscure the true ownership structure. Beneficial Owner data reported to the Ministry of Law and Human Rights then becomes part of the legal administration system that can be accessed by relevant authorities, including law enforcement agencies and financial institutions, for monitoring and law enforcement purposes (KPK, 2025).

The primary function of BO reporting is not only to fulfill administrative obligations but also as part of efforts to prevent and eradicate Money Laundering (TPPU). In many cases, criminals use legal entities as a tool to disguise the origins of illicit funds, such as proceeds from corruption, drug trafficking, or other economic crimes (Maulidah et al., 2024). By providing transparency regarding who the BO is, authorities can more easily trace the flow of funds and identify responsible parties. Furthermore, this system is also in line with international standards set by the Financial Action Task Force (FATF), which emphasizes the importance of ownership transparency as a key pillar of anti-money laundering and counter-terrorism financing regimes.

One major problem is the emergence of the phenomenon of “shadow controllers.” This term refers to individuals or parties who de facto control a legal entity but are intentionally not listed in official BO reports, *Shadow controller. They* typically operate behind the scenes by exploiting various loopholes in the legal and administrative systems. They may use nominees or other parties as formal owners, construct complex ownership structures through multiple layers of companies, or use specific powers to control companies without being registered as owners (Putri et al., 2025).

The phenomenon of *shadow control* demonstrates the difference between formal ownership and actual control. In many cases, the parties listed as shareholders or company managers are merely "puppets" acting on behalf of others. Meanwhile, the shadow controller, the party with actual control, remains behind the scenes and untouched by the official reporting system (Nov, 2016). This is certainly a serious problem, as the primary goal of ownership transparency is undermined. Instead of disclosing information, the BO reporting system can be manipulated to create a false sense of compliance.

The negative impacts of shadow controllers are extensive and complex. One of the most obvious impacts is the increased risk of tax evasion. By concealing the identity of their true owners, shadow controllers can divert profits to other parties or jurisdictions to reduce tax liabilities (Sr, 2023). Furthermore, this phenomenon also opens up significant opportunities for money laundering. Funds derived from illegal activities can be channeled through seemingly legitimate legal entities, making them difficult for authorities to trace. In more extreme cases, shadow controllers can also be involved in terrorism financing or corrupt practices, directly impacting economic stability and national security.

In practice, many BO reports are not updated regularly, resulting in outdated and irrelevant information. Furthermore, the initially reported data may be inaccurate or even intentionally manipulated. For example, a company may report a specific BO to fulfill an administrative obligation, but in reality, control of the company has passed to another party that is not reported.

In such situations, the role of financial institutions, particularly banks, becomes crucial. Banks hold a strategic position as intermediaries in the financial system, allowing

them to interact directly with various parties in daily transactions. In many cases, banks possess more up-to-date information about who actually controls a legal entity because they can directly observe transaction patterns, relationships between parties, and customer behavior. This makes banks "gatekeepers" with a significant responsibility for maintaining the integrity of the financial system.

As *gatekeepers, b*anks should not solely rely on BO data available from the Ministry of Law and Human Rights. While this data is important as an initial reference, banks must conduct further verification and analysis to ensure that the information reflects actual conditions. This aligns with the prudential principle that underpins banking operations. In the context of preventing money laundering, banks are required to implement a Customer Due Diligence (CDD) process, a series of steps to identify and verify the identity of customers, including beneficial owners of legal entities. This process includes gathering information on the ownership structure, the purpose of opening an account, and the customer's risk profile.

However, in certain cases with higher risk levels, implementing CDD alone is not sufficient. Banks must conduct Enhanced Due Diligence (EDD). EDD, as defined by POJK Number 8 of 2023, is a more in-depth CDD action carried out by financial service providers on prospective customers, WICs, or customers who are high risk, including PEPs and/or in high-risk areas, such as more in-depth and comprehensive examinations of customers or transactions deemed suspicious. EDD can include analysis of funding sources, business relationships with other parties, and ongoing transaction monitoring. Through EDD, banks can identify indications of shadow controllers, for example, when there is a party that consistently provides transaction instructions but is not listed as an owner or manager of the company.

It's important to understand that detecting shadow controllers isn't always easy. In many cases, these entities deliberately create complex structures to evade detection. Therefore, banks need to develop a more proactive and risk-based approach. Beyond relying on formal documentation, banks must also leverage technology and data analytics to identify unusual patterns. For example, using transaction monitoring systems to detect activity inconsistent with customer profiles or network analysis to identify hidden connections between various parties.

Furthermore, cooperation between banks and authorities is also a crucial factor in increasing the effectiveness of shadow controller detection. Banks can report suspicious transactions to relevant institutions, allowing for further investigation. In this context, banks' role extends beyond simply acting as business actors, but also as part of a broader oversight system. Therefore, efforts to prevent money laundering and terrorism financing are not solely dependent on a single institution, but are the result of collaborative efforts across multiple parties.

Thus, it can be seen that although the regulation regarding beneficial owner reporting administered by the Ministry of Law and Human Rights has provided a strong foundation for increasing transparency, various challenges remain in its implementation. The phenomenon of shadow controllers demonstrates that loopholes remain that can be exploited to conceal the identity of true owners. The gap between formal data and the reality on the ground demonstrates that the beneficial owner reporting system is not yet fully effective in achieving its objectives.

In this context, the role of banks as gatekeepers is crucial. Banks not only serve as transaction intermediaries but also as parties capable of detecting and preventing financial system abuse. Therefore, banks must take an active role by comprehensively implementing Customer Due Diligence and Enhanced Due Diligence, and not relying solely on available

administrative data. With a more proactive and risk-based approach, banks can become the first line of defense in identifying the presence of shadow controllers.

Synergy between the government, financial institutions, and other relevant parties is needed to ensure that the objectives of BO reporting are truly achieved. This is expected to make Indonesia's financial system more transparent, accountable, and resilient to various forms of abuse, thereby supporting sustainable economic development with integrity.

The problem formulation in this study focuses on the legal liability of banks when they fail to detect the presence of shadow controllers not listed in the Beneficial Owner (BO) report. The main problem formulation is the extent to which banks can be held accountable if they are unable to identify the party that actually controls a legal entity. This is important because banks hold a strategic position as parties that interact directly with customers' financial activities. If banks rely solely on formal data from the Ministry of Law and Human Rights without conducting further analysis, the potential for overlooking shadow controllers is quite high. Therefore, failure to detect this can be seen as a form of negligence in implementing the principle of prudence.

Second, how banks can be sanctioned if they ignore indications of a shadow controller. These sanctions can be administrative, such as fines or warnings, but they can also extend to civil and criminal matters, particularly when related to money laundering. In this context, it's also important to understand the concept of "should have known" or constructive knowledge, which is the condition under which a bank is deemed to have been aware of irregularities if it had followed proper procedures, for example, by analyzing transaction patterns or unusual ownership structures.

The purpose of this article is to analyze the basis of bank responsibility under applicable regulations and to provide recommendations so that banks do not rely solely on BO reports from the Ministry of Law and Human Rights. This discussion is important for banking practitioners, compliance officers, and regulators in strengthening early detection systems for shadow controller risks.

2. RESEARCH METHODS

This research uses a normative legal research method or literature study, namely, research conducted by examining library materials or secondary data without conducting field surveys. The sources of legal materials used consist of three categories (Satresna, 2023). Primary legal materials include laws and regulations that are still in effect today, namely Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 and last amended by Law Number 4 of 2023 concerning Development and Strengthening of the Financial Sector (P2SK), Law Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes, Financial Services Authority Regulation Number 8 of 2023 concerning Implementation of Anti-Money Laundering Programs, Prevention of Terrorism Financing, and Prevention of Proliferation of Weapons of Mass Destruction Financing in the Financial Services Sector; Regulation of the Minister of Law Number 2 of 2025 concerning Verification and Supervision *Beneficial Owner* Corporations; and Regulation of the Minister of Law Number 49 of 2025 concerning Procedures for the Establishment, Amendment, and Dissolution of Limited Liability Companies. Secondary legal materials include banking law textbooks, scientific journals, legal articles, and relevant court decisions. Tertiary legal materials, such as legal dictionaries, are used to understand technical terms. The data collection technique is carried out through literature studies by searching legal databases such as JDIH, Google Scholar, and trusted journal portals. Data analysis uses a normative qualitative analysis method with a statutory approach (*statute approach*) and a conceptual approach (*conceptual approach*).

The validity of research results is guaranteed through the principles of relevance and authenticity of sources, as well as *cross-check* between primary and secondary legal materials.

3. RESULTS AND DISCUSSION

1. Bank's Legal Responsibility for Detecting *Shadow Controller* in BO Report

Bank's legal liability for failure to detect *shadow controllers,* which are not listed in the report, *Beneficial Owner* (BO) must essentially be viewed within the legal obligations inherent in banks as financial intermediaries. In the Indonesian legal system, banks function not only as collectors and distributors of funds but also have a responsibility to maintain the integrity of the financial system. This dual position places banks at the forefront of efforts to prevent various forms of financial crime, including money laundering, terrorism financing, and tax evasion (Setiono et al., 2022). This responsibility is not merely a matter of business ethics but is expressly stipulated in various legally binding regulations.

Banks' obligations are reflected in various regulations, particularly Law Number 7 of 1992 concerning Banking, as most recently amended by Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK), as well as provisions related to the prevention of Money Laundering (TPPU). The P2SK Law, which has been in effect since 2023, brings significant changes to the regulation of the financial sector, including strengthening banks' obligations to identify customers and report suspicious transactions (Sanarta, 2024). These changes are a response to the increasingly complex dynamics of financial crime, including the modus operandi of *shadow controllers,* which are difficult to detect. In this regulation, banks are required to apply the principle of prudence (*prudential principle*), one concrete form of which is the application of the principle of *Know Your Customer* (KYC) and *Customer Due Diligence* (CDD).

The principle of prudence is the primary foundation of banking operations in Indonesia. This principle requires banks to pursue more than just profit but also to consider the risks that may arise from each business relationship. In the context of detection, the *shadow controller, the* principle of prudence requires banks to remain vigilant against the possibility of third parties secretly controlling legal entity customers (Perwirasari & Ikrardini, 2020). Failure to implement this principle can have fatal consequences, not only for the bank itself but also for the stability of the financial system as a whole. Therefore, regulators place compliance with the prudential principle as one of the main indicators of bank health.

Through KYC and CDD principles, banks are required to fully recognize customer identities, including understanding who the actual beneficial owners or controllers of a legal entity are. This provision is emphasized in regulations issued by the Financial Services Authority through OJK Regulation Number 8 of 2023 concerning the Implementation of the Anti-Money Laundering and Prevention of Terrorism Financing (APU-PPT) Program. POJK 8/2023 is a very comprehensive technical regulation, regulating in detail how banks must identify, verify, and monitor customers (Ben et al., 2025). In this regulation, banks are not only required to formally identify customers, but also must understand the ownership and control structure, including the *beneficial owner.* This means that banks have an active obligation to gather information, not simply accept data provided by customers or rely solely on administrative documents.

This active obligation is often referred to as the principle of *"customer risk profiling"* or customer risk mapping. Banks are required to be more than passive and

formalistic, but rather to dig deep into the information. For example, when dealing with a legal entity with a multi-level ownership structure, banks should not be satisfied with just knowing the name of the ultimate shareholder. Banks must continue to trace upwards until they find the individuals who truly enjoy the economic benefits of the legal entity (Cesarianti, 2025). This tracing process requires high analytical skills and perseverance, because *shadow controllers* often design complex structures to avoid detection.

In this context, Banks' responsibilities do not stop at matching data with the BO report submitted to the Ministry of Law and Human Rights (Kemenkumham). Although the BO report is an official source of information managed by the state, banks are still required to conduct independent verification and analysis. This is important because BO reports can, in practice, be inaccurate, out of date, or even intentionally manipulated by dishonest legal entity owners. Data from the Ministry of Law and Human Rights is only one source of information, not the only source of truth. A good bank must be able to do this *cross-check* between official data and other information obtained from various sources, such as interviews with company management, visits to business premises, or analysis of other public archives.

Therefore, if there is an indication that the party controlling the company is different from that listed in the BO report, the bank should take further steps, such as a more in-depth examination (*Enhanced Due Diligence or* EDD). EDD is a more intensive procedure than the regular CDD, which is applied to high-risk customers. In EDD, banks must collect additional information, such as the source of wealth (*source of wealth*) and sources of funds (*source of funds*), from customers, verify submitted documents, and monitor transactions more strictly and continuously. Failure to perform EDD when required could constitute negligence in fulfilling legal obligations. Regulators may determine that banks should have been aware of the need for more in-depth audits, but ignored them for efficiency or business reasons.

The concept of bank responsibility in this situation can also be understood through the approach of *gatekeeper liability*, namely the responsibility as a "gatekeeper" in the financial system. As *gatekeeper* Banks have a strategic role in preventing the entry of illegal funds into the financial system. In this position, banks are expected to be not only passive but also proactive in detecting and preventing potential misuse. If banks fail to carry out this function, especially when there are clear signs of the existence of... a *shadow controller*, then the bank can be considered not to have fulfilled its legal obligations as a *gatekeeper*. Draft *gatekeeper liability. It* has actually been known for a long time in the common law legal system, and has begun to be adopted in various regulations in Indonesia, especially those related to preventing money laundering.

However, it is important to understand that the bank's legal responsibility is not absolute (*strict liability*). In the Indonesian legal system, in general, the bank's responsibility is more directed towards *fault-based liability* or liability based on fault. This means that a new bank can be held responsible if it can be proven that there is an element of fault, either in the form of negligence (*negligence*) or intentional *misconduct*. This approach reflects the principle of justice that a person or corporation should not be punished without proving fault. In this context, the concept of "should have known" (*constructive knowledge*) becomes very important. If, under certain conditions, the bank should be able to know that there is a *shadow controller*, for example, through unusual transaction patterns, the presence of a dominant party in decision-making, or a complex ownership structure, then failure to detect this can be considered negligence.

On the other hand, if a bank has carried out all its obligations in accordance with applicable standards, such as conducting CDD and EDD adequately, documenting the entire process properly, and finding no suspicious indications despite conducting professional analysis, it is difficult to declare that the bank has committed a violation. In other words, the bank's responsibility depends heavily on the extent to which the bank has met the prudential and compliance standards set by regulations. Therefore, the assessment of a bank's legal responsibility must be carried out on a case-by-case basis, taking into account the available facts and evidence (Maluw et al., 2024). There is no single approach, *one size fits all, in* determining whether a bank is negligent or not.

2. Legal Sanctions for Ignoring Indications of Existence: *Shadow Controller*

Banks that ignore indications of the presence of shadow controllers can essentially be subject to various forms of legal sanctions, including administrative, civil, and criminal sanctions, depending on the severity of the error and the resulting impact. Under the Indonesian legal framework, banks' obligations to recognize customers and identify beneficial owners are part of the implementation of the prudential principle and the Anti-Money Laundering and Prevention of Terrorism Financing (AML-CFT) program (Reedy, 2023). This obligation is stipulated in various regulations, including the Banking Law, the Law on Money Laundering Crimes, and technical provisions from the Financial Services Authority (OJK) through POJK Number 8 of 2023. In this context, a bank's failure to detect shadow controllers can be considered a violation of compliance obligations.

From Sisi's administrative sanctions, Banks can be subject to various forms of action by supervisory authorities if they are proven to have failed to properly comply with AML-CFT obligations. These administrative sanctions can include written warnings, fines, restrictions on business activities, and even revocation of business licenses in serious cases. In practice, banking and AML-CFT regulations authorize regulators to impose sanctions in stages according to the severity of the violation (Lawsonline Publication Team, 2026). For example, under Bank Indonesia and the Financial Services Authority (OJK) regulations, violations of reporting obligations or the implementation of AML-CFT procedures can result in financial fines and written warnings. Furthermore, POJK 8 of 2023 emphasizes the importance of active supervision by directors and commissioners, as well as the obligation to have an adequate internal control system. If a bank fails to meet these standards, administrative sanctions are a natural consequence.

Furthermore, from a civil perspective, banks also have the potential to be sued by parties harmed by their negligence in detecting shadow controllers. For example, if a company is found to be controlled by a hidden party committing fraud or misappropriation of funds, third parties such as creditors, investors, or business partners could suffer losses. In such circumstances, the bank could be held jointly liable if it is proven not to have properly carried out its due diligence obligations. These civil lawsuits are usually based on unlawful acts (PMH), where the bank is deemed negligent in carrying out its obligations, resulting in losses for another party. In other words, even if the bank is not the primary perpetrator, its negligence in detecting risks can still give rise to legal liability.

In addition to administrative and civil sanctions, there is also the possibility of imposing criminal sanctions, especially if there is an element of intent or gross negligence. Law Number 8 of 2010 concerning Money Laundering stipulates that any party who knows or reasonably suspects a suspicious transaction but fails to report it

may be subject to criminal sanctions. (Long & Wulan, 2025). The concept of "reasonably suspected" here aligns with the principle of constructive knowledge, which refers to the condition under which a party should have known there were indications of a violation. If bank management or employees deliberately ignore signs of a shadow controller, for example, by continuing to facilitate suspicious transactions, this could be classified as a criminal act. In fact, under certain circumstances, criminal liability can be imposed not only on individuals but also on the bank corporation as a legal entity.

In practice, although the term "shadow controller" is not always explicitly used, numerous cases demonstrate that negligence in implementing AML-CFT can result in serious sanctions. For example, there are cases where financial institutions have been fined by regulators for failing to detect suspicious transactions or report potentially money laundering-related activities. This demonstrates that supervisory authorities assess not only formal compliance but also the effectiveness of internal oversight systems. In other words, banks need not simply have procedures on paper; they must also be able to implement them in practice.

3. Standard of Proof: *Constructive Knowledge* Bank against *Shadow Controller*

Standard of proof, *constructive knowledge,* or "should have known" in the context of the bank's responsibility for the existence of a *shadow controller,* is an important issue in banking law and the Money Laundering prevention regime. Simply put, *constructive knowledge does* not require any real knowledge (*actual knowledge*), but assesses whether a party, in this case the bank, should have known a fact if it had carried out its obligations properly and reasonably. In the Indonesian legal system, this concept is not always explicitly stated, but is reflected in various provisions, such as the phrases "should have known" or "should have suspected," which are widely used in laws and regulations, including in Law Number 8 of 2010 concerning Money Laundering (TPPU). These phrases indicate that the law assesses not only what is actually known, but also what should have been known based on applicable professional standards.

In the banking context, this standard is closely related to the obligation to apply the principle of prudence (*prudential principle*) and the obligation to identify customers through Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) as regulated by the Financial Services Authority (OJK) in POJK Number 8 of 2023 concerning AML-PPT. This regulation emphasizes that banks must understand the customer's comprehensive profile, including ownership and control structures, and monitor transactions continuously (Ritiau & Baidhowi, 2025). Therefore, if there is a strong indication of a party controlling the company but not listed in the Beneficial Owner report at the Ministry of Law and Human Rights, the bank should be able to detect it through an adequate analysis process. Failure to recognize this can be considered negligence if objective indicators are already available.

To prove that the bank "should have known" about the existence of a *shadow controller*, objective indicators that can be tested legally are needed. One of the most common indicators is the presence of suspicious transactions that don't match the customer profile. For example, a small company suddenly makes large or frequent transactions inconsistent with its business activities. In AML-CFT practice, such a situation should trigger an alert of *red flag and* encourage the bank to conduct further analysis. If the bank ignores a clearly unusual transaction pattern, then this can be the basis for the bank having *constructive knowledge* of the potential existence of hidden parties controlling the transaction.

The second indicator is a complicated or non-transparent ownership structure. Many *shadow controllers use* layered schemes, such as shell companies or nominees, to hide their identities. In this situation, the bank has an obligation to not only accept the structure as it is, but also to assess its reasonableness and purpose (Red, 2016). If the ownership structure appears too complex without a clear business rationale, then this should be a signal for the bank to take action *enhanced due diligence*. Failure to follow up on these indications may be considered negligence, because the bank is not carrying out its obligations optimally.

The third indicator is a discrepancy between official documents, such as beneficial owner reports, and the customer's operational reality. For example, the official document states that the company owner is A, but in daily practice, it is B who gives instructions, transactions, makes important decisions, or communicates with the bank as the dominant party. This condition is one of the clearest signs of *shadow controller* (Napitupulu, 2025). If banks continue to ignore these operational facts and rely solely on formal documents from the Ministry of Law and Human Rights, they may be deemed to be failing to adhere to the principle of prudence.

Furthermore, regarding the burden of proof, in both criminal and administrative cases, the burden of proof essentially rests with the public prosecutor or regulator alleging a violation. However, in the banking context, there is a tendency for a limited reversal of the burden of proof, particularly in cases related to money laundering. This means that banks also have an obligation to demonstrate that they have implemented CDD and EDD procedures in good faith. If a bank can demonstrate that all procedures have been carried out according to standards, this can form the basis for a defense that they were not negligent (Jayanti, 2025). Conversely, if the bank's documentation and internal processes reveal deficiencies or omissions, this would strengthen the argument that the bank "should have known" about the violation.

In assessing whether a bank has fulfilled its obligations, the principle of *reasonableness* or fairness becomes very important. This principle assesses whether the bank's actions are in accordance with the standards that should be carried out by a professional and prudent bank assessment, which is objective, meaning it not only examines the bank's subjective intentions but also compares these actions with common practices in the banking industry (Yanto, 2025). If, under similar circumstances, another reasonable bank would conduct further investigations, a bank's failure to do so may be considered unreasonable and potentially give rise to legal liability.

Thus, the standard of proof *constructive knowledge* in the context of an existence *shadow controller* depends not only on whether the bank actually knew, but more on whether it should have known based on existing indicators. The combination of regulatory obligations, objective indicators, and the principle of fairness is the primary basis for assessing a bank's responsibility. Therefore, banks are required not only to comply formally but also to be active and critical in analyzing each risk, thereby preventing abuse of the financial system by parties attempting to hide behind seemingly legitimate formal structures.

4. Case study

The Panama Papers and Jiwasraya Scandal cases are two important events that illustrate how weak the transparency of beneficial ownership can open up space for the emergence of hidden controllers in the financial system. The Panama Papers, revealed in 2016, stemmed from the leak of millions of documents from the Panamanian law firm Mossack Fonseca, which exposed the practices of global use of (*shell companies*) to hide the identity of the true owner. Wealthy individuals, politicians, and

multinational corporations utilize layered ownership structures using nominee directors and nominee shareholders so that the names formally listed are not the ones with actual control. In practice, banking institutions continue to facilitate the opening of accounts and financial transactions for these companies, despite indications that information regarding beneficial owners is not transparent. This situation indicates weaknesses in the application of the principle of *Know Your Customer* (KYC) and *Customer Due Diligence* (CDD), which should enable banks to identify risks early on, including detecting the presence of parties acting as *shadow controllers*.

Meanwhile, in the Jiwasraya case, which emerged in the period 2018 to 2020 in Indonesia, the chronology of the PT Asuransi Jiwasraya (Persero) case. PT Asuransi Jiwasraya, established on December 31, 1859, is a state-owned company engaged in life insurance services with the aim of providing protection and financial planning to the public. However, since mid-2018, indications of fraud and manipulation in financial reporting by company management have resulted in losses for the state and millions of customers. This problem stemmed from the JS Saving Plan product, which offered unrealistic returns of 9–13 percent per year, far above bank deposit interest rates. This product attracted public interest, but in reality, customer funds were not managed prudently. The problem arose from the state-owned insurance company's failure to meet its payment obligations to customers, triggered by large investment losses. Investments were made in high-risk stocks affiliated with certain parties, raising suspicions of strong influence from parties not formally registered within the company structure but who exercised control over investment decision-making. This pattern indicates the existence of a *shadow controller*, a party that de facto controls corporate activities without being listed as an official owner or manager. In practice, all of Jiwasraya's financial activities, including investment transactions and cash flows, still involve the banking system as an intermediary, so banks are strategically positioned to detect unusual transaction patterns. However, if banks do not conduct an in-depth analysis of affiliate relationships and ownership structures, the potential existence of these hidden controllers will go undetected.

From an Indonesian legal perspective, the obligation to identify and report beneficial owners is regulated in Presidential Regulation Number 13 of 2018 concerning the Implementation of the Principle of Recognizing Beneficial Owners of Corporations, which requires every corporation to disclose beneficial owners to the state through the General Legal Administration (AHU) system of the Ministry of Law and Human Rights. In addition, Law Number 10 of 1998 concerning Banking emphasizes that banks are required to implement the principle of prudence (*prudential banking principle*) in all their business activities, including receiving and processing customer transactions. This obligation is reinforced by Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU), which requires banks to continuously identify, verify, and monitor customer transactions and report suspicious transactions to the Financial Transaction Reports and Analysis Center (PPATK). In this context, banks are not only administratively responsible but can also be held legally accountable if proven negligent in implementing KYC, CDD, and other principles *enhanced due diligence* (EDD), especially when there are strong indications of concealment of the identity of the beneficial owner.

Thus, both cases show that the existence of a *shadow controller* is a real risk that can arise from a lack of transparency in corporate ownership structures. In the Panama Papers, weaknesses in the global system allowed the concealment of beneficial owners' identities through shell companies, while in Jiwasraya, weak governance and oversight

allowed certain parties to control strategic decisions without formal recording. In both situations, banks should play an active role at the forefront of detecting and preventing financial system abuse through optimal application of prudential principles. Therefore, strengthening the implementation of regulations related to beneficial ownership and data integration between financial institutions and the government is a crucial step to ensure that the true controllers of a corporation can be accurately identified, thereby minimizing the risk of financial loss and legal violations.

4. CONCLUSION

Based on the discussion regarding the legal responsibility of banks in detecting *shadow controllers, r*egarding those not listed in the Ministry of Law and Human Rights' Beneficial Owner (BO) report, three main conclusions can be drawn. First, the bank's legal responsibility for failure to detect a *shadow controller* of a nature *fault-based liability* (responsibility based on fault), not *strict liability*. Banks are required to apply the principles of *Know Your Customer* (KYC), *Customer Due Diligence*(CDD), and the principle of prudence as stipulated in Law Number 7 of 1992 concerning Banking, which was last amended by Law Number 4 of 2023 concerning P2SK and POJK Number 8 of 2023 concerning APU-PPT. Banks may not only rely on BO reports from the Ministry of Law and Human Rights, but are required to conduct independent verification and analysis. Second, banks that ignore indications of the existence of a *shadow controller.* Three types of sanctions can be imposed. Administrative sanctions include warnings, fines, and even business license revocation. Civil sanctions include a lawsuit for damages based on unlawful acts. Criminal sanctions, based on Law Number 8 of 2010 concerning Money Laundering (TPPU), apply to bank managers who intentionally or negligently fail to report suspicious transactions. Third, the standard of proof *constructive knowledge* (should know) banks is based on objective indicators: suspicious transactions, complex ownership structures without clear business reasons, and discrepancies between official BO report documents and the customer's operational reality. The assessment uses the principle of fairness (*prudent banker*). If the indicator appears but is ignored, the bank is deemed to have known about its *shadow controller and* can be held legally accountable. Banks must act proactively as *gatekeeper* financial system.

5. BIBLIOGRAPHY

Ben, B., Silalahi, S., & Novita, Y. D. (2025). Aspek Hukum Dalam Penerapan Prinsip Know Your Customer (KYC) Pada Lembaga Perbankan. *Media Hukum Indonesia (MHI)*, *2*(6), 399–406.

Cesarianti, F. M. (2025). Analisis Yuridis Penerapan Prinsip Mengenal Nasabah (Know Your Customer) sebagai Upaya Penanggulangan Tindak Pidana Pencucian Uang pada Perusahaan Asuransi (Studi Putusan Nomor 538 / PID . SUS / 2023 / PN . Jkt . Sel). *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, *2*(2).

Jayanti, H. D. (2025). *Kaji CDD dan EDD untuk Nasabah Berisiko Tinggi sebagai Strategi Mitigasi Risiko Keuangan*. Hukum Online. https://www.hukumonline.com/berita/a/kaji-cdd-dan-edd-untuk-nasabah-berisiko-tinggi-sebagai-strategi-mitigasi-risiko-keuangan-lt67dd1bcfb1135/

KPK. (2025). *KPK: Transparansi Data Beneficial Ownership Berperan Penting Cegah Terjadinya Korupsi*. Komisi Pemberantasan Korupsi. https://www.kpk.go.id/id/ruang-informasi/berita/kpk-transparansi-data-beneficial-ownership-berperan-penting-cegah-terjadinya-korupsi

Long, T. K., & Wulan, E. R. (2025). DASAR HUKUM YANG DI TETAPKAN HAKIM

DALAM KASUS TINDAK PIDANA PENCUCIAN UANG. *Iblam Law Review*, *5*(2).

Maluw, S. J., Tampongangoy, G. H., & Korah, R. S. M. (2024). PENERAPAN PRINSIP KEHATI – HATIAN BANK BERBASIS DIGITAL DALAM MEMBERIKAN KREDIT KEPADA DEBITUR. *Jurnal Fakultas Hukum UNSRAT Lex Administratum*, *12*(2).

Maulidah, K., Hengki, M. R., & Sari, R. K. (2024). PERTANGGUNGJAWABAN PIDANA PEMILIK MANFAAT (BENEFICIAL OWNER) DALAM TINDAK PIDANA PENCUCIAN UANG. *IBLAM LAW REVIEW*, *4*(2).

Napitupulu, D. R. W. (2025). *BUKU AJAR HUKUM PERBANKAN DAN JAMINAN*. UKI PRESS.

Nov. (2016). *Direktur-Direktur "Boneka" Ini Ungkap Permainan Proyek Nazar*. Hukum Online.

Perwirasari, D. P., & Ikrardini, Z. (2020). PENERAPAN PRINSIP KEHATI-HATIAN DALAM DITINJAU DARI SISI HUKUM PERIKATAN (Studi Kasus Pada PT . Bank Negara Indonesia (Persero) Tbk . *Jurnal Dialektika Hukum*, *2*(2), 148–172.

Pradhana, A. P., Chairani, M. A., & Yitawati, K. (2025). PERKEMBANGAN REGULASI MENGENAI BENEFICIAL OWNERSHIP DI INDONESIA BAGI KORPORASI DALAM BISNIS DAN PENCEGAHAN TINDAK PIDANA. *Jurnal Magister Hukum PERSPEKTIF*, *16*(2).

Putri, S. H. M., Widyastari, D. N. A. C., Esa, P. Y., Nasoetion, D. N., Ismi Kinanthi Isnani, J. N. S., & Taufik, M. (2025). Piercing the Corporate Veil Sebagai Instrumen Pertanggungjawaban Pidana Korporasi dalam Kejahatan Deforestasi : Analisis Normatif Kritis Terhadap Penegakan Hukum Lingkungan di Indonesia. *Journal Evidence Of Law*, *4*(3), 2221–2231.

Red. (2016). *Begini Modus Law Firm dan Bank Bantu Klien Sembunyikan Aset*. Hukum Online. https://www.hukumonline.com/berita/a/begini-modus-law-firm-dan-bank-bantu-klien-sembunyikan-aset-lt5704c9da001e2/

Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*(January), 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

Ritiau, E. J., & Baidhowi. (2025). PERAN PERBANKAN DALAM PENCEGAHAN TINDAK PIDANA PENCUCIAN UANG. *Jurnal Hukum Dan Kewarganegaraan*, *13*(5).

Sanarta, K. (2024). *Ini 5 Perubahan UU OJK dalam UU 4/2023 yang Wajib Diketahui Pelaku Jasa Keuangan*. Hukum Online. https://rcs.hukumonline.com/insights/perubahan-uu-ojk

Satresna, D. P. (2023). Pengaturan Metode Omnibus Dalam Undang-Undang Nomor 13 Tahun 2022 Tentang Pembentukan Peraturan Perundang-Undangan. *Japhtn-Han*, *2*(1), 63–80. https://doi.org/https://doi.org/10.55292/japhtnhan.v2i1.68

Setiono, G. C., Rahman, I., & Ananfa, E. D. (2022). Tanggung jawab bank sebagai wujud perlindungan hukum bagi nasabah kontrak perbankan. *Jurnal Transparansi Hukum*, *5*(1), 66–79.

Sr, N. P. D. (2023). *Shadow Economy, Ini Dampak Buruknya Jika Tak Ditangani*. Pajakku. https://artikel.pajakku.com/shadow-economy-ini-dampak-buruknya-jika-tak-ditangani

Tim Publikasi Hukumonline. (2026). *Menjawab Tantangan APU-PPT di Sektor Jasa Keuangan: Dari Kewajiban Regulasi ke Praktik Kepatuhan yang Efektif*. Hukum Online. https://www.hukumonline.com/berita/a/menjawab-tantangan-apu-ppt-di-

sektor-jasa-keuangan--dari-kewajiban-regulasi-ke-praktik-kepatuhan-yang-efektif-lt6985ccd016c2f/

Yanto, R. (2025). Implementasi Penerapan Pengaturan Bank Dengan Prinsip Kehati Hatian (Prudent Banking) Di Indonesia. *Global Intellectual Community of Indonesia Journal*, *2*(1), 21–27.